CYBERPOWER AS A COERCIVE INSTRUMENT

BY

MAJOR ANN M. HALLE

A THESIS PRESENTED TO THE FACULTY OF

THE SCHOOL OF ADVANCED AIR AND SPACE STUDIES

FOR COMPLETION OF GRADUATION REQUIREMENTS

SCHOOL OF ADVANCED AIR AND SPACE STUDIES

AIR UNIVERSITY

MAXWELL AIR FORCE BASE, ALABAMA

JUNE 2009

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
JUN 2009	**N/A**	**-**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Cyberpower As A Coercive Instrument	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **School Of Advanced Air And Space Studies Air University Maxwell Air Force Base, Alabama**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES
The original document contains color images.

14. ABSTRACT

This thesis aims to help bridge the gap between existing knowledge of cyberspace and the practical use of cyberpower as a coercive instrument. This knowledge will assist leaders at all levels to properly integrate cyberpower into a well-crafted strategy. This analysis demonstrates that although cyberpower has potential as an effective coercive instrument, it requires further evolution to be a persistent and powerful force by itself. This study examined the details of nine separate cyber attacks against the United States, Estonia, and Georgia. Cyberpower failed to deter or compel in the cases examined. The research question of this study is, Can cyberpower coerce adversarial states and non-state actors? This study concludes that used alone, cyberpower has yet to show coercive ability. Used in a combined campaign with other instruments, it also has yet to prove its coercive ability. However, cyberpower can be effective in brute force actions, both alone and when combined with other instruments.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**SAR**	**75**	

APPROVAL

The undersigned certify that this thesis meets masters-level standards of research, argumentation, and expression.

_____

MAJOR IAN BRYAN (Date)

_____

DR. JOHN B. SHELDON (Date)

DISCLAIMER

The conclusions and opinions expressed in this document are those of the author. They do not reflect the official position of the US Government, the Department of Defense, the United States Air Force, or Air University.

ABOUT THE AUTHOR

Major Ann M. Halle is a senior pilot with over 16 years of active service. She is a C-17A instructor pilot with over 2800 hours in the T-37, T-1, and C-17A aircraft. Most recently Major Halle served as the Chief of Safety, 376th Air Expeditionary Wing, Manas Air Base, Kyrgyzstan. She received the Air Education and Training Command Flight Safety Officer of the year award for 2007. She graduated in 1995 from Embry-Riddle Aeronautical University with a B.S. in Professional Aeronautics and in 1996 with an M.A. in Professional Aeronautics. Following graduation from the School of Advanced Air and Space Studies, Major Halle will be Branch Chief of the Special Warfare Doctrine Division at the Air Force Le May Doctrine Center, Maxwell AFB, Alabama.

ACKNOWLEDGEMENTS

I would like to thank Major Ian Bryan and Dr. John Sheldon for their critical analysis of my work. Their insight and patience has been invaluable in designing the concepts needed to explain a somewhat enigmatic topic. The intellectual heavy lifting involved with this thesis was a true challenge. I also owe a debt of gratitude to Class XVIII. Without their exhortation and commentary the thoughts contained in this paper would be far less vibrant.

I would be remiss if I did not extend thanks to Major General Michelle Johnson and the action officers in the Chairman of the Joint Chiefs of Staff, Joint Staff Cyberspace Operations and Policy Directorates. Their work in this nascent area of military operations served as a guide and inspiration for this thesis.

Finally, it is hard to quantify the debt of gratitude I owe to my children, sweet Brooke and Beau. To my children I say, I love you and thank you for supporting my efforts -- its all for you. To my ex-husband, thank you for the support you gave me. To my parents, thank you for your undying support and mentoring both this year and all the years of my life. To the other members of my family, my close-knit group of friends, and my boyfriend, I give my utmost gratitude for your support, love, and guidance throughout this challenging academic year. I could not have made it without you.

ABSTRACT

This thesis aims to help bridge the gap between existing knowledge of cyberspace and the practical use of cyberpower as a coercive instrument. This knowledge will assist leaders at all levels to properly integrate cyberpower into a well-crafted strategy.

This analysis demonstrates that although cyberpower has potential as an effective coercive instrument, it requires further evolution to be a persistent and powerful force by itself. This study examined the details of nine separate cyber attacks against the United States, Estonia, and Georgia. Cyberpower failed to deter or compel in the cases examined. The research question of this study is, "Can cyberpower coerce adversarial states and non-state actors?" This study concludes that *used alone, cyberpower has yet to show coercive ability. Used in a combined campaign with other instruments, it also has yet to prove its coercive ability. However, cyberpower can be effective in brute force actions, both alone and when combined with other instruments.*

TABLE OF CONTENTS

Chapter Page

ILLUSTRATIONS

Table

Figure

Introduction

The information technology revolution continues to improve people's lives. However, societies and governments are becoming more reliant on information technology while the means to disrupt this hardware and information flows are proliferating. States and non-state actors are in the early phases of figuring out how to wield new information technologies as an element of power and more specifically, a weapon.

The elements of national power have shifted throughout history and we are witnessing such a shift today. For instance, when society was agriculturally-based, a country would aim to gain control over the land. When society was industrially-based, a country would aim for control over the means of natural resources.[1] Today, society is information-based. So, countries are now vying for control over cyber infrastructures.[2]

Cyber-dependence makes nations vulnerable. If an adversary gains control of critical parts of a nation's cyber infrastructure it can put modern society at risk. These include financial networks and databases, air and ground transportation systems, power stations, power grids, water and sewage networks, the Internet, satellite, cellular, and land-based communication, and navigation networks. These vulnerabilities occur in all cyber-dependent states so, it is useful for the strategist to understand how coercion works under these circumstances. This thesis aims to help bridge the gap between existing knowledge of cyberspace and the practical use of cyberpower as a coercive instrument. This knowledge will assist leaders at all levels to properly integrate cyberpower into strategy.

This analysis demonstrates that although cyberpower has potential as an effective coercive instrument, it requires further evolution to become a persistent and powerful force. This study parses out the details of nine separate cyber attacks against the US, Estonia, and Georgia. Overall, cyberpower failed to deter or compel in the cases examined.

---

[1] Alvin and Heidi Toffler, *War and Anti-War: Survival at the Dawn of the 21st Century* (London: Little, Brown, 1993), 29-85.
[2] Dan Verton, *Black Ice: The Invisible Threat of Cyber-Terrorism* (New York, NY: McGraw-Hill Professional, 2003), 182.

Cyberpower has shortcomings as a coercive instrument. To use cyberpower for deterrence or compellence requires cyberpower to serve as the basis for a credible threat. Cyberpower has yet to reliably show this capability. Since cyber attack methods are susceptible to rapidly-developed, low cost countermeasures, cyberpower lacks persistence.[3] Without persistence, it cannot show strategic or long-term effectiveness. Another shortcoming of cyberpower is the unknown political and economic implications that can arise when using cyberpower to coerce. More study is required to know the possible unintended collateral damages and unacceptable consequences that can result from cyber attacks.

Cyberpower, however, shows potential as a coercive instrument. Coercion is the manipulation of an enemy's cost-benefit calculus so as to lead the target entity to make choices the coercer desires. Cyberpower has the potential to punish an adversary. Cyberpower also has advantages other weapons do not have, such as anonymity and deniability. Some adversaries might find that useful for sparking war between third parties by commandeering command and control systems.

This study is organized into five chapters and a conclusion. Chapter one provides definitions for key terms and explains basic coercion theory. Chapters two, three, and four are case studies of the cyber attacks on the US, Estonia, and Georgia. Each chapter looks closely at the effectiveness of cyberpower used as a coercive force. Chapter five wraps up with an in-depth analysis of the previous chapters and future implications for the use of cyberpower as a coercive instrument.

---

[3] Akin to the *paradox of strategy* illustrated by Edward N. Luttwak in his book, *Strategy: The Logic of War and Peace*, coercion via cyberpower is paradoxical. In most forms of warfare, coercion (deterrence and compellence, as discussed in chapter one) is best performed overtly. With cyber attacks, as soon as a cyber attack method is used, an immediate response-in-kind can be formulated by the opponent. Accordingly, multiple cyber attack methods must be available to ensure preparation for defense when planning offensive cyber attacks. Herein lies the paradox. If the aggressor conducts a cyber attack, he/she shows the method of attack upon use. If an aggressor wants to deter, he/she must prove ability to attack. If an aggressor wants to compel, he/she must prove ability to punish. However, if he/she attacks, the specific method(s) of attack required to punish may be immediately used against him/her in a response-in-kind from the opponent. Hence, the paradox of cyber attack strategy is an important concept to understand if planning to utilize cyberpower as a coercive instrument. See Edward N. Luttwak, *Strategy: The Logic of War and Peace*, (Cambridge, MA: Harvard University Press, 2002), 87-91. The concepts in this paragraph derived from personal interviews with CIA and FBI Cyber Investigation Experts in Langley and McClean, VA, and US Chairmen of the Joint Chiefs of Staff, Joint Staff, Cyberspace Operations and Policy Action Officers and Directors, 29 March – 1 April 2009.

Chapter 1

Cyber Terms and Coercion Theory

This chapter defines cyber terms relevant to coercion and then describes coercion theory and its constituent parts: deterrence and compellence. These terms and theory are the foundation for the case studies and analysis within the following chapters.

Cyber Terms

Cyber terms relevant to this study include cyber, cyberspace, cyber infrastructure, cyberpower, and cyber warfare. A great deal of confusion surrounding cyberspace stems from a misunderstanding of its core terminology.

"Cyber" is a modern prefix, meaning "of, relating to, or involving computer networks (and the Internet)."[1] When combined with the word "space," it has become a common reference to anything dealing with computers and the Internet.

A useful definition for "cyberspace" must have specificity. At the same time, it should reflect the global and contiguous nature of cyberspace, as well as its non-contiguous parts. The definition of cyberspace also should refer to the electromagnetic spectrum. The small band of the electromagnetic spectrum which cyberspace uses is the physical feature of cyberspace that is not visible to the naked eye. Cyberspace cannot exist without it. In Rebecca Grant's report, "Victory in Cyberspace," she describes cyberspace as, "… a single medium, but (it) has multiple theaters of operation."[2] Martin Libicki writes in his book, *Conquest in Cyberspace,* that cyberspace is "the sum of the globe's communication links and computational nodes."[3] Gregory Rattray provides a broader definition in his book, *Strategic Warfare in Cyberspace*, "Cyberspace, however, is actually a physical domain resulting from the creation of information systems and

[1] Encarta World English Dictionary [North American Edition] 2009, http://encarta.msn.com/encnet/features/dictionary/DictionaryResults.aspx?refid=1861671109, (accessed: 5 May 2009).
[2] Rebecca Grant, "Victory in Cyberspace," *Air Force Association,* October 2007, 3.
[3] Martin C. Libicki, "The Emerging Primacy of Information," *Orbis,* Volume 40, Issue 2, (Spring 1996): 261-274.

networks that enable electronic interactions to take place."[4] Another definition to consider comes out of the US National Military Strategy for Cyberspace Operations, which states, "Cyberspace is a global domain characterized by the use of electronics and the electromagnetic spectrum to store, modify, and exchange data via networked systems and associated physical infrastructures."[5] These definitions may be useful, but none combines the features of specificity, scope, and emphasis on the electromagnetic spectrum to meet the requirements of this study.

US Air Force Cyberspace doctrine combines the required features for the definition of cyberspace needed in this study. It states that, "Cyberspace is a global domain consisting of the interdependent network of information technology (IT) infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[6] It further delineates cyberspace as "a domain characterized by the use of electronics and the electromagnetic spectrum to store, modify, and exchange data via networked systems and associated physical infrastructures."[7] Cyberspace is a man-made domain, and is therefore unlike the natural domains of air, land, and sea. It requires continued attention from humans to persist.[8] Thus, these statements combine to encompass the features of specificity, global scope, and emphasis on the electromagnetic spectrum.

Even though networks in cyberspace are interdependent, parts of these networks are isolated (Figure 1). Isolation in cyberspace exists via protocols, firewalls, encryption, and physical separation from other networks. For instance, classified networks such as the US armed forces Secure Internet Protocol Router net (SIPRnet) are not hardwired to the Internet at all times, but connect to it via secure portals. Additionally, the construction of some hard-wired networks isolates them from most forms of radio frequency (RF) interference. These factors enable these networks to be isolated within cyberspace, yet still allow controlled connectivity to global networks.

---

[4] Gregory J. Rattray, *Strategic Warfare in Cyberspace*, (MIT Press, 2001), 17.
[5] US Department of Defense. *National Military Strategy for Cyberspace Operations (NMS-CO)*, (Washington D.C.: Joint Staff, 2006), ix.
[6] Air Force Doctrine Document (AFDD) 2-11, *Cyberspace Operations*, (draft) (Air Force Doctrine Center, 2009), 1.
[7] AFDD 2-11, 58.
[8] AFDD 2-11, 3.

Cyberspace exists via a cyber infrastructure serving as the converging place of physical infrastructure, electronic systems, and the electromagnetic spectrum (Figure 2). A sampling of networks within cyberspace is listed in Table 1.

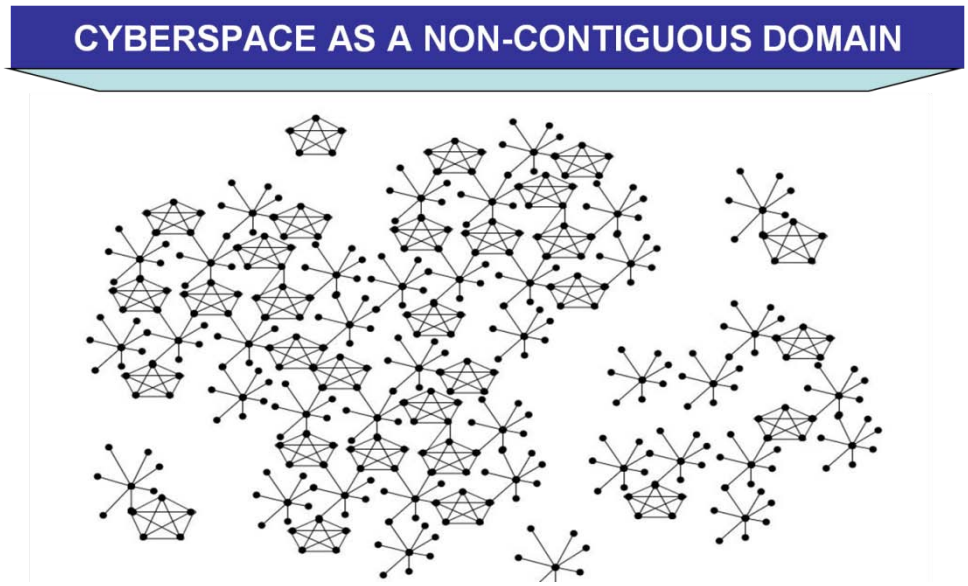

Figure 1. Cyberspace as a Non-Contiguous Domain
AFDD 2-11, 6

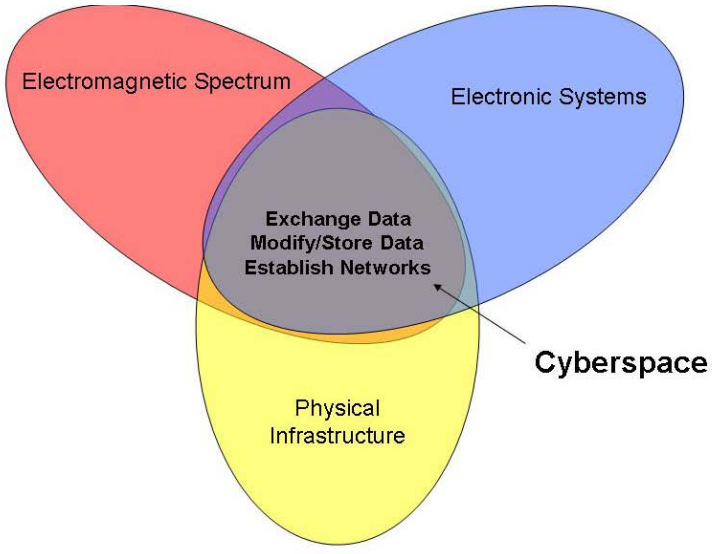

Figure 2. Cyberspace
AFDD 2-11, 4.

Cyberpower is the capability to control networks in cyberspace. Table 1 illustrates the various ways that networks in cyberspace relate to each other. The key elements of cyberpower are, "the science of the electromagnetic spectrum, the technology of electronics, and integrated manmade infrastructure."[9] The key aspect of cyberpower is its capability to manipulate or access a target's cyber infrastructure via exploitation and attack. This includes the simultaneous maintenance of a defensive posture. When applying cyberpower, there is a range of ability to manipulate or access a target's cyber infrastructure. More cyberpower applied (more effective malicious code, multiple attacks/exploits, longer lasting attacks/exploitation, etc…) equals more ability to manipulate or access and vice versa. Means of cyberpower come via cyber warfare.

Table 1: Example Networks in Cyberspace

Franz, Timothy P. *IO Foundations to Cyberspace Operations: Analysis, Implementation Concept, and Way Ahead for Network Warfare Forces.* Wright-Patterson Air Force Base, OH: Air Force Institute of Technology, Department of Electrical and Computer Engineering, 2007.

IP-based Communication Networks - Internet - NIPRNet, SIPRNet, etc. - Voice Over IP (VOIP) Telephony Systems - Banking Infrastructure	Closed-network Battlefield Systems - Integrated Air Defense Systems (IADS) - Tactical Data Information Links (TADIL) - C^2 Networks
Distributed Control Systems - Supervisory Control and Data Acquisition/Control Systems (SCADA/CS) - Manufacturing Process Control Systems - Energy Generation and Distribution Systems	Tactical Communication Networks - Theater Airborne and Terrestrial Radio Systems - Mobile Radios (cell phones, mobile data services) - Land Mobile Radio (LMR) (first responder, law enforcement, local C2 networks)
Transportation Control Systems - Regional or Global Air Traffic Control (ATC) Systems - Airfield Air Traffic Control and Landing Systems (ATCALS)	Global Communications Networks - Satellite Communications Networks (SATCOM) - Fiber Optic Networks - Telephony - Global Positioning Systems

Cyber warfare is the use of cyberpower to either inflict or threaten punishment against an adversary, or to achieve political objectives through brute force without the

[9] US Department of Defense. *Air Force Cyber Command Strategic Vision.* (Washington D.C.: Air Force, 2007), 7-8.

enemy's acquiescence.[10] Cyberpower relies on hardware and software. Hardware is the mechanical, magnetic, electronic, and electrical devices comprising a computer system, such as the CPU, disk drives, keyboard, or screen. Cables, satellites, routers, computer chips, and the like are also considered hardware. Software consists of the programs used to direct computer operations and uses.[11] Malware is malicious software that interferes with normal computer and Internet-based application functions and is a key weapon in cyber warfare.[12]

Cyber warfare often involves units organized for offensive and defensive cyber warfare operations. Units like these are often state sponsored. "Cyber corps and cyber warriors are terms often used in reference to US government personnel who conduct cyber operations."[13] The US has dedicated specialized portions of its armed forces to codify cyber warfare doctrine, provide education, and perform cyber warfare operations. Similarly, the People's Liberation Army of China has formulated official cyber warfare doctrine, implemented appropriate training for its officers, and conducted cyber warfare simulations and military exercises.[14] State sponsored units like these conduct cyber warfare via the Internet today.

Some hackers are state sponsored and perform lawful activities, but some are not. Both kinds can be instrumental in the conduct of cyber warfare. Hackers have expertise in software programming and manipulation. They concentrate their actions on exploiting the intricacies of computer networks. "Hacktivist" is a common term for hackers who use illegal digital tools in pursuit of political ends.[15] When cyber warfare operators conduct cyber attacks for authorized state sponsored attacks and use legal means, they are considered to be legal hackers. Legal hackers conduct cyberspace operations under legal authority for legal purposes with no adversarial intent. For instance, cyber security experts deliberately hack into computer networks to find inherent weaknesses. Members

---

[10] Lech Janczewski and Andrew M. Colarik, *Cyber Warfare and Cyber Terrorism*, (Idea Group Inc, Hershey, PA, 2007), xiv.
[11] Merriam-Webster, *Collegiate Dictionary*, 1186.
[12] Malware. Dictionary.com. The American Heritage® Dictionary of the English Language, Fourth Edition. Houghton Mifflin Company, 2004. http://dictionary.reference.com/browse/malware (accessed: March 22, 2009).
[13] Stephen W. Korns and Joshua E. Kastenberg, "Georgia's Cyber Left Hook," *Parameters*, Winter 2008-09, 20-73.
[14] Charles Billo and Welton Change, *Cyber Warfare: An Analysis of the Means and Motivation of Selected Nation States*, Thesis (Hanover: Institue for Security Technology Studies at Dartmouth College, 2004), 1-10.
[15] These tools include web site defacements, redirects, denial of service attacks, malware, information theft, web site parodies, virtual sit-ins, virtual sabotage, and software development. See AFDD 2-11, 1.

of the armed forces and government intelligence operatives also deliberately hack into military computer networks to find vulnerabilities. They also can act as adversarial hackers to test defensive and offensive abilities. These hackers are either industry or government-sponsored and are not hacking for personal gain. If hackers are attempting to gain access into computer networks, etc… for the sake of political gain, it can part of a state-sponsored campaign. Additionally, other hackers conduct cyber operations on behalf of personal political causes such as the environment, human rights, and animal rights. Albeit, the actual hacking activities may still be covert in nature – depending on the operation at hand – but what determines the legality of these operations is intent. Even covert state-sponsored operations can be considered legal since the purpose is not personal gain. Therefore, if the cyber attacks on Georgia – discussed in chapter 4 – were indeed sponsored by the Russian government, then these hackers' operations can be considered legal. On the other hand, when hackers have malicious intent to their activities and are hacking specifically for personal or non-state sponsored political gain, they may be considered as political hackers (hacktivists) or criminal hackers.[16]

Defining cyber terms in this section has laid the foundation for understanding the cyber attacks discussed in the following chapters. The purpose of this study is to discover cyberpower's effectiveness when used as a coercive instrument of power. The next section describes basic coercion theory, which will be the framework for analyzing the case studies.

Coercion Theory

Coactus volui, tamen volui.
I willed under coercion, but still I willed.
–Old Roman Jurist Saying

Coercion is the act of manipulation using deterrence, compellence, or both. This section seeks to summarize basic coercion theory, while acknowledging the fact that other interpretations exist. Daniel Byman and Matthew Waxman, authors of *The*

[16] Information considering the legality of cyber attacks and legal versus illegal hackers gathered from personal interviews with CIA and FBI Cyber Investigation operatives, 30 March – 1 April 2009. Also, see Samuel Arwood, "Cyberspace as a Theater of Conflict: Federal Law, National Strategy and The Departments of Defense and Homeland Security" Graduate Research Project, Wright-Patterson Air Force Base, OH: Air Force Institute of Technology, Department of Electrical and Computer Engineering, 2007.

Dynamics of Coercion: American Foreign Policy and Limits of Military Might, define coercion as "getting an adversary to act in a certain way via anything short of brute force; the adversary must still have the capacity for organized violence but choose not to use it."[17] Robert Pape mentions, in his book *Bombing to Win: Airpower and Coercion in War*, that coercion also includes "efforts to change the behavior of a state by manipulating costs and benefits," in addition to brute force.[18] Another theorist, Lawrence Freedman, defines strategic coercion slightly differently. He states that deterrence is the, "deliberate and purposive use of overt threats to influence another's strategic behavior."[19] Beyond coercion, brute force actions are available to force a target's compliance.

Coercion involves the manipulation of a target's behavior (Figure 3). Coercion consists of two categories: deterrence and compellence.[20] Both deterrence and compellence focus on influencing the target's decision-making via threats. Brute force, on the other hand, forces the target to comply via shear exertion of physical power or strength. The target does not have a choice to make.

Important to coercion is a threat of action or threat of continued action. Key factors of a credible threat include capability, commitment, and clear communication. Part of making a threat credible is clearly communicating a threat to the target. A threat is credible when the target perceives the coercer as capable of and committed to carrying out the threat. The coercee may see the threat of future punishment as more credible after the coercer has inflicted some punishment on the coercee. Thomas Schelling writes, in *Arms and Influence*, "…the hurting does no good directly, as it can only work indirectly. Coercion depends more on the threat of what is yet to come than on damage already done." He goes on to say, "Unless the object is to shock the enemy into sudden submission, the military action must communicate a continued threat."[21] Therefore, it is not the initial punishment or cost that makes a threat credible. What makes a threat

[17] Daniel Byman and Matthew Waxman, *The Dynamics of Coercion: American Foreign Policy and the Limits of Military Might* (Cambridge: Cambirdge University Press, 2002), 3.
[18] Robert A. Pape, *Bombing to Win* (Ithaca, NY: Cornell University Press, 1996), 4.
[19] Lawrence Freedman, *Strategic Coercion: Concepts and Cases* (Oxford: Oxford University Press, 1998), 3.
[20] Thomas C. Shelling, *Arms and Influence* (London: Yale University Press, 1966), 69-91.
[21] Shelling, *Arms and Influence*, 172.

credible is the coercee's belief in the coercer's ability and commitment to carry out any future punishment or cost.

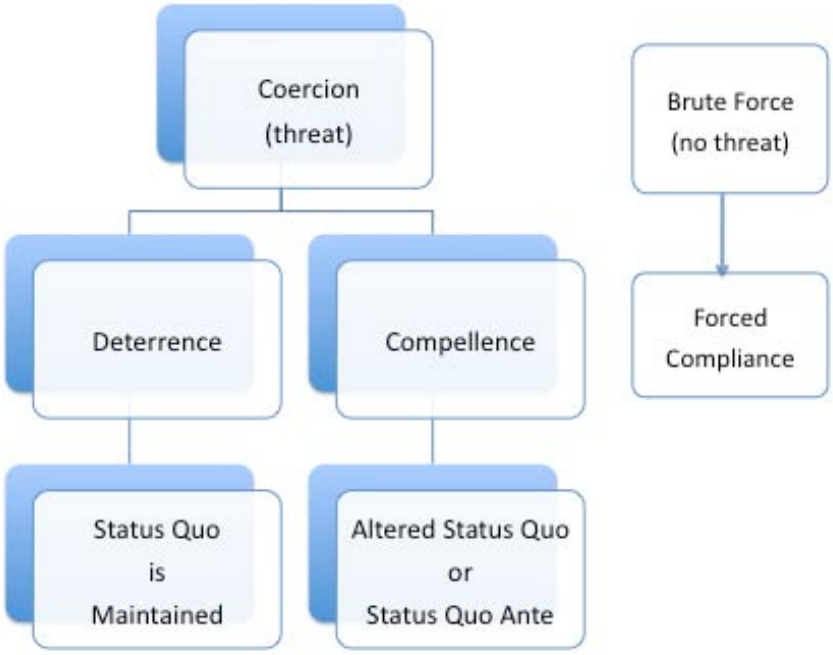

Figure 3. Coercion

Other authors, such as Thomas C. Shelling and Robert A. Pape differ slightly in their interpretations of coercion. This author has created this diagram to pictorially portray her working definition for the purposes of this study.

Deterrence seeks to maintain the status quo by discouraging a target from changing its behavior. Deterrence has its roots in the Latin word *deterre,* meaning to frighten from or away.[22] It involves attempts to prevent unmaterialized action from occurring in the first place.[23] In his book, *Deterrence,* Lawrence Freedman observed, "Deterrence is the deliberate attempt to manipulate the behavior of others through conditional threats."[24] Compellence, on the other hand, takes a different approach.

Compellence seeks to force the target to change the status quo.[25] Compellence, therefore, is about inducing a target to choose an action desired by the coercer. Compellence is the flip side of deterrence, but is linked in practice. At the same time the coercer hopes to convince the target to change its behavior, the target can hope to deter the coercer from executing the threat. Compellence, like deterrence, relies on threats of

[22] Freedman, *Deterrence*, 7.
[23] Byman and Waxman, *The Dynamics of Coercion*, 6.
[24] Freedman, *Deterrence*, 6.
[25] According to Thomas C. Shelling, the goal of compellence could also be to change the target's behavior back to the original status quo, or a different status quo, chosen by the coercer.

punishment to manipulate an adversary's cost-benefit calculus and induce an adversary to either change or maintain the status quo, depending on the coercer's preference.

Whereas coercion involves persuading an adversary to make a choice, brute force is the label applied to actions meant to rob the adversary of any choice and directly achieve an object. In other words, the enemy does not have the choice not to comply. The aggressor takes what it wants without requiring the target's compliance. Brute force actions do not rely on threats.

In conclusion, chapter one has examined terminology and theory relevant to examining cyberpower as a coercive instrument. It defined working definitions of cyber, cyberspace, cyber infrastructure, cyberpower, and cyber warfare. It parsed out the basics of coercion theory to include deterrence and compellence. It also explained brute force actions in relation to coercion. Chapters two, three, and four contain case studies of nine cyber attacks in the US, Estonia, and Georgia. Chapter five follows with an analysis of cyberpower in terms of coercion theory in light of the case studies.

Chapter 2

Cyberpower Attacks on the United States

A source of power for the US is its vast cyber infrastructure, enabling US citizens to be highly cyber-dependent. The vast cyber infrastructure of the US includes over 7,000 Internet Service Providers (ISPs).[1] With a population of over 307 million, the US is highly dependent on cyber-based capabilities with over 223 million Internet users. Therefore, the US is vulnerable to cyber attack, yet more challenging to attack when compared to smaller countries. This case study examines seven cyber attacks on the US cyber infrastructure between 1998 and 2009. These attacks are: Solar Sunrise, Code Red, Mountain View, Nimda, Slammer, Titan Rain, and Conficker.

To ensure clear understanding and facilitate the analysis of the case studies presented within this thesis, each case study uses a common framework. To organize the analysis of this case study of the cyber attacks on the US, prominent features of these cyber attacks include timing, suspected aims, duration, and resultant effects. An exacerbating factor to the apparent strategic ineffectiveness of these attacks is the vast size of the US cyber infrastructure. To strategically affect a cyber infrastructure of this magnitude, an adversary will have to discover methods that can affect both contiguous and non-contiguous networks.[2] None of the attacks against the US cyber infrastructure studied here performed these tasks in any persistent manner. The actual aim and perpetrator of most of the attacks is unknown. The duration of each attack was short, with most lasting less than one month. Resultant effects were not strategic in scope. Most of the attacks seemed unable to affect the massive US cyber infrastructure in any long-term or severe way.

---

[1] Infoplease: all the knowledge you need, 2009, http://www.infoplease.com/ipa/A0108121.html, (accessed 27 April 2009).

[2] An adversary can decide to affect only the contiguous networks that are interconnected in cyberspace and forgo targeting the non-contiguous networks with the dependent factor being the adversaries intended target. Or, the adversary can decide to narrow the method of attack to only one type of network. If the chosen target of the cyber attack includes both types of network, the methods of attack must be amended accordingly. If it includes only one type, then the methods can be more narrowly focused.

Solar Sunrise

During the month of February 1998, US Department of Defense computer networks experienced a series of cyber attacks. The attacks were codenamed Solar Sunrise. These attacks, eleven in total, hit US Air Force, Navy, and Marine Corps unclassified computer networks worldwide. The attackers gained administrator system privileges. The attacks appeared to originate in the United Arab Emirates, France, Taiwan, and Germany. The actual perpetrators were two teenage hackers, one Israeli and one American.[3] It remains unclear whether or not the teenagers were working alone or as adversarial state-sponsored hackers.

The pattern of these widespread and systematic cyber attacks indicated exploitative intent. Many cyber attacks gather information and data by spying on cyber infrastructures. The opponent uses the information and data collected to take advantage and exploit the opponent. Adversaries use cyber attacks for the purpose of finding vulnerabilities in cyber infrastructures and develop ways to compromise cyber infrastructure. The Solar Sunrise attacks exploited well-known system vulnerabilities and followed the same profile with each attack: 1) probe the system, 2) exploit the system, 3) implant a sniffer program into the system, and 4) return later to gather data the sniffer program collected from the system. The sniffer programs targeted key ports and gathered hundreds of network passwords.[4] If the hackers responsible for Solar Sunrise were indeed state-sponsored, the aim could have been to test methods for future cyber attacks on the US Defense Information Infrastructure.

Since these eleven intrusions gained unauthorized access to the command and control computer networks of the US armed forces, they pose a threat to US national security. In context, during February 1998, tensions between the US, the UN, and Iraq were high.[5] The cause of concern was that breaches of this type could affect the deployment of US military forces to the Middle East. Because of quick action by the US to investigate the intrusions, no critical information was lost.[6] UN weapon inspections

---

[3] Roderic G. Broadhurst and Peter N. Grabosky, *Cyber-crime*, (Hong Kong, Hong Kong University Press, 2005), 330-333.
[4] Solar Sunrise, *Global Security Organization*, http://www.globalsecurity.org/military/ops/solar-sunrise.htm, (accessed: 11 April 2009).
[5] Kenneth M. Pollack, *The Threatening Storm: The Case for Invading Iraq* (New York: Random House, 2002), 87-94.
[6] Broadhurst and Grabosky, *Cyber-crime*, 330-333.

continued, Operations Northern and Southern Watch continued, and the US went to war with Iraq in 2003. This event highlighted the fact that "understanding of the critical infrastructure's threat environment is barely in its infancy."[7]

Code Red

On 19 July and 6 August 2001, worms named Code Red I and Code Red II infected over 359,000 US computers in just under 14 hours.[8] The Cooperative Association for Internet Data Analysis (CAIDA) estimated damage caused by Code Red to exceed $2.6 billion.[9] This worm was time sensitive. Within infected computers, it performed pre-programmed distributed denial of service (DDoS) network attack functions against various websites only on the 20-27th days of every month. At all other times, it remained dormant within infected computers.[10] According to the book, *The Next War Zone,* written by military news analyst James Dunnigan, the websites defaced by the worm broadcast a message that read "Hacked by Chinese."[11] He mentions that information embedded in the defaced websites led analysts to also believe a part of Code Red I would self-activate on 31 July 2001.

To put this cyber attack in context, in April 2001 Chinese hacker groups started a popular worldwide cyber movement to deface US websites. Their motivation came from the crash of a Chinese fighter jet following a collision with an American patrol plane. At first, the Chinese hackers experienced counter-attacks by pro-American hackers. The American hackers successfully defeated the Chinese attackers at a ratio of three to one. The Chinese hackers retaliated with the release of the first of two Code Red Worms. The worms originated at the Chinese University in Guangdong, China. The Chinese government continues to proclaim its belief that in the arena of cyber warfare, it can achieve first-rate capability as a near-peer competitor to the United States.[12]

---

[7] Broadhurst and Grabosky, *Cyber-crime*, 332.
[8] Bernadette Hlubik Schell and Clemens Martin, *Cybercrime*, (Oxford, UK, ABC-CLIO,, 2004), 15. And Harold F. Tipton and Micki Krause, *Information Security Management Handbook, Edition: 6*, (Boca Raton, FL, CRC Press, 2007), 77.
[9] Harold F. Tipton and Micki Krause, *Information Security Management Handbook, Edition: 6*, (Boca Raton, FL, CRC Press, 2007), 405.
[10] The Spread of the Code Red Worm, *CAIDA: The Cooperative Association for Internet Data Analysis*, David Moore and Colleen Shannon, 18 November 2008, http://www.caida.org/research/security/code-red/coderedv2_analysis.xml, (accessed 8 March 2009).
[11] James F. Dunnigan, *The Next War Zone*, (Charleston, SC, Citadel Press, 2003), 79.
[12] Dunnigan, *The Next War Zone*, 91.

One of Code Red's specific targets was the US President's White House website. Code Red activated itself at 8 PM, 31 July 2001. US Presidential cyber security experts frustrated this attack. They prevented the DDoS of the White House website by blocking Internet traffic to it at the server. Ron Dick, former Director of the Federal Bureau of Investigation's (FBI) National Infrastructure Protection Center, commented on the attack, "This attack is a great example of where a system administrator had not applied a patch."[13]

This cyber attack advertized enemy capabilities. This version of malware might seem harmless since it only resulted in website defacements. Actually, it did more than that. This cyber attack proved the capability to shut down websites on demand. It showed the speed at which a worm could infiltrate Internet-based networks within cyberspace. By the end of July 2001, there were perhaps "a million servers that were still vulnerable and capable of being turned into Net-choking, spamming machines" by the Chinese-based Code Red worm.[14] Wartime versions of Code Red, or similar malware, are not likely to make their presence known until they are unleashed to spread their original brand of denial or destruction.[15] The Code Red attacks are similar to the attacks on Estonian and Georgian presidential websites to be discussed in chapters three and four.

Mountain View, CA

Another cyber espionage[16] attack occurred during the summer of 2001 against the cyber infrastructure of Mountain View, CA. The unknown adversary probed the city's websites and computer networks. The FBI traced the source back to locations in the Middle East and Southeast Asia. The adversary gathered information on the city's

[13] Interview, Frontline, "Cyber War!," 18 March 2003, http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/warnings/, (accessed: 5 March 2009).
[14] Dunnigan, *The Next War Zone*, 80.
[15] Dunnigan, *The Next War Zone*, 80.
[16] Cyber espionage is not the same as passive espionage. Spying in cyberspace often causes damage to the system or network it is spying on. Therefore, it attacks the system it is spying on. The introduction of harmful information (making espionage possible) into a networked system can cause the system to error (for example, by causing it to confuse authorized vs. unauthorized users). In the world of computer network operations, cyberespionage falls under the umbrella of computer network exploitation (one of the three joint computer network operations - the other two are computer network attack and defense). Computer network exploitation is the art of extracting information from a system against the will of its owners. Computer exploitation operations (having freedom to conduct espionage within cyberspace) frustrate the working controls of network authorization systems. See Martin C. Libicki, *Conquest in Cyberspace: National Security and Information Warfare* (Cambridge, NY: Cambridge University Press, 2007), 38.

utilities, government offices, and emergency systems.[17] Richard Clarke, US Presidential Advisor for Cyber Security, spoke of this event, "The bottom line on the Mountain View case is the ease with which people can do virtual reconnaissance from overseas on our physical infrastructure. We were lucky in the case of Mountain View that there were good people watching."[18]

The suspected aim of this intrusion was preparation for future cyber attacks.[19] The timing of the intrusions in Mountain View, CA is suspect since they occurred in the fall of 2001.[20] The adversary gathered critical information about the inner workings of the city's cyber infrastructure. The adversary only spied on the network. There was no evidence of resultant damage to the computers or networks. Was this meant to be a show of force or a just another test by adversarial cyber forces in preparation for future attacks? The FBI attempted to find the answer.[21]

During their investigation of the intrusions on Mountain View's city government cyber infrastructure, the FBI found some disturbing information. This attack seemed to be a test of feasible uses of Information and Communication Technology (ICT) to launch attacks on cyber infrastructure. They found "multiple casings of sites" stemming from Saudi Arabian, Indonesian, and Pakistani sources. The casings focused on 911 emergency systems, electrical and nuclear power grids, water systems, and natural gas facilities. The casings also focused on other critical parts of US national cyber infrastructure systems, specifically remotely controlled utility systems. When the FBI seized Al Qaeda computers in 2004, they found data related to these casings on the hard drives.[22] The Mountain View cyber intrusions were significant because they opened up the possibility of a major cyber attack against critical infrastructure by a terrorist

---

[17] Barton Gellman, "Cyber-Attacks by Al Qaeda Feared," *The Washington Post.com*, 27 June 2002, http://www.washingtonpost.com/wp-dyn/content/article/2006/06/12/AR2006061200711.html, (accessed: 11 May 2009).
[18] Frontline, "Cyber War!," http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/warnings/, (accessed: 5 March 2009).
[19] This conclusion derived from personal interview with US Chairman of Joint Chiefs of Staff, Joint Staff, Cyberspace Operations and Policy Division Action Officers and Directors, 30 March 2009, Pentagon, Washington, DC.
[20] Barton Gellman, "Cyber-Attacks by Al Qaeda Feared," *The Washington Post.com*, 27 June 2002, http://www.washingtonpost.com/wp-dyn/content/article/2006/06/12/AR2006061200711.html, (accessed: 11 May 2009).
[21] Antonino Zichichi, Richard C. Ragaini, Ettore Majorana International Centre for Scientific Culture, *International Seminar on Nuclear War and Planetary Emergencies, 31st Session*, (Hackensack, NJ, World Scientific, 2004), 391.
[22] Barton Gellman, "Cyber-Attacks by Al Qaeda Feared," *The Washington Post.com*, 27 June 2002, http://www.washingtonpost.com/wp-dyn/content/article/2006/06/12/AR2006061200711.html, (accessed: 11 May 2009).

organization, as well as uncertainty about how much information about the command and control arrangements of US critical infrastructure had fallen into terrorist hands.

Nimda

On 18 September 2001, as the US was still reeling from the September 11th terrorist attacks, the Nimda worm attacked the US cyber infrastructure. It is possible to conceive that the adversary responsible used the diversion of the terrorist attacks to facilitate flooding cyberspace with Nimda. "A virtual Swiss Army knife of exploits, this new worm appeared to spread by multiple vectors."[23] It carried five different malicious payloads via e-mail.[24] It automatically infected every computer it met. This worm did not exploit by planting any new programs in computers. Instead, it exploited existing vulnerabilities embedded in Microsoft software. It scanned systems for over 100 vulnerabilities. This worm exploited open doors left behind in computers infected with the Code Red worm.[25] After discovering vulnerabilities, it immediately exploited them. After only thirty minutes, it was a worldwide problem. The Nimda worm subsequently caused the Internet to slow down after infecting millions of computer networks.[26]

Nimda reached far within US open networks. Hardest hit were financial industry databases and computer networks.[27] After the attack, the director of Information Assurance Strategic Initiatives for Computer Sciences Corporation's Homeland Security program and former director of the FBI's National Infrastructure Protection Center, Ron Dick mentioned, "It proliferated across the world at a far greater rate than Code Red did. It rattled the backbone of the Internet. It caused billions of dollars in damage from stolen information, corrupted data, and system downtime. And we still don't know who proliferated that virus."[28] Richard Clarke described the events on the day of the attack as follows, "Nimda was a devastating attack…the cyber security team came to me and said there was a major worm going through the Internet and it was knocking off major

---

[23] Jay Beale, Brian Caswell, James C. Foster, Jeffrey Posluns, Ryan Russell, *Snort 2.0 Intrusion Detection*, (Rockland, MA, Syngress 2003), 24.
[24] Jay Beale, et al., *Snort 2.0 Intrusion Detection*, 11.
[25] Lance Spitzner, *Honeypots: Tracking Hackers*, (Old Tappan NJ Addison-Wesley, 2003), 22.
[26] Verton, *Black Ice*, 159-161.
[27] Frontline, "Cyber War!," http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/warnings/, (accessed: 5 March 2009).
[28] Frontline, "Cyber War!," http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/warnings/, (accessed: 5 March 2009).

companies."[29] In a later interview on 5 December 2001, Mr. Clarke mentioned, "We still don't know for sure, but had Nimda happened prior to September 11th, it would have been a big news story. Many companies, particularly in the financial world, shut down major pieces of their operations. It destroyed and corrupted databases. It was quite devastating, causing several billion dollars in damage."[30]

The Nimda worm demonstrated various cyber warfare methods, but did not appear to have coercive intent. Its unique multi-vector approach included e-mail, Internet, and computer network attacks. It was the first worm of its kind that combined these methods and used files to infect other files. The Nimda worm cannot be considered a method of using cyberpower to coerce for two reasons. One, there was no attributable threat issued. Two, there was no clear intent of behavioral change demanded or communicated by any adversary. However, Nimda did perform a brute force act of cyberpower in that it denied services across the US cyberinfrastructure.

Slammer

Two years after Nimda came the Slammer worm cyber attack. This attack was the fastest and most effective worm to date. Its injection into the Internet started at roughly midnight on 25 January 2003. It took roughly three minutes to travel the globe and infected over 300,000 servers.[31] Slammer, known to some as the Sapphire worm, was similar to Nimda since it also exploited existing Microsoft software vulnerabilities.[32]

The most notable far-reaching effects of this attack were the denial of services in South Korea and Japan, disruption of phone services in Finland, and slow airline reservations and automatic banking services in the US.[33] Richard Clarke said, "The worm could have been much more damaging. It could have been attached to a destructive payload. The fact that it wasn't leads me to think that it may have been a test to see what damage could have been done. Next time, it might have a very destructive

[29] Verton, *Black Ice*, 160.
[30] Verton, *Black Ice*, 160.
[31] Hussein Bidgoli, *Handbook of Information Security: Threats, Vulnerabilities, Prevention, Detection, and Management*, (Hoboken, NJ, John Wiley and Sons, 2006), 226..
[32] Harold F. Tipton and Micki Krause, *Information Security Management Handbook, Edition: 6*, (Boca Raton, FL, CRC Press, 2007), 2849.
[33] Bidgoli, *Handbook of Information Security*, 29.

payload."[34] The Slammer worm affected the usability and viability of 911 networks and banking operations.[35] President George W. Bush's number two cyber security adviser, Howard Schmidt, acknowledged that the "collateral damage" of this attack had uncertain effects on the nation's most important electronic systems.[36]

The actual intent of this cyber attack was unknown. Had it carried a destructive payload, it could have had similar effects to the Nimda worm. Attacks of this type could be a form of long-term posturing by adversaries of the US and other NATO member states. The cyber attacks on Georgia discussed in chapter four examine this concept more closely. In essence, if cyber war causes enough destruction to a member state's cyber infrastructures, NATO could employ security measures. These measures would extend NATO protective powers and support to any member state experiencing cyber attacks. The fear of future attacks of this type can undermine general belief in national cyber infrastructure security and ultimately, the government responsible for ensuring that security.

Titan Rain

On the night of 1 November 2005, a Chinese-based cyber attack, codenamed Titan Rain, infiltrated and mapped US armed forces computer networks. Titan Rain specifically targeted multiple military networks in quick fashion. At 10:23 pm, it hit the US Army Information Systems Engineering Command at Fort Huachuca, Arizona. By 1:19 am, it found the same vulnerability within computers at the Defense Information Systems Agency in Arlington, Virginia. At 3:25 am, it infected the Naval Ocean Systems Center, in San Diego, California. Finally, the attack stopped at 4:46 am, after finding the same vulnerability at the United States Army Space and Missile Defense installation in Huntsville, Alabama.[37] The night of 1 November 2005 was a dark night for US

---

[34] Frontline, "Cyber War!," http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/warnings/, (accessed: 5 March 2009).
[35] Peter Abraham, "The Slammer Worm Attack: The worst attack to date, probably not the last," *Dynamic.net News*, 14 February 2003, http://dynamicnet.net/news/articles/slammer.html, (accessed 5 March 2009).
[36] Peter Abraham, "The Slammer Worm Attack: The worst attack to date, probably not the last," *Dynamic.net News*, 14 February 2003, http://dynamicnet.net/news/articles/slammer.html, (accessed 5 March 2009).
[37] Nathan Thornburgh, "Inside the Chinese Hack Attack," *Time* , 25 August 2005, http://www.time.com/time/nation/article/0,8599,1098371,00.html, (accessed: 28 March 2009).

Department of Defense (DoD) unclassified networks. This attack proved the existence of exploitable vulnerabilities and security holes in these networks.

All of the computer systems affected by this attack were unclassified and directly connected to the Internet. Even so, these attacks gathered enormous amounts of information.[38] According to Major General William Lord, US Air Force, "China has downloaded 10 to 20 terabytes of data from the NIPRNet (DoD's Non-Classified Internet Protocol Router Network)."[39] No attacks occurred on classified computers, most likely because classified computers usually have no direct Internet connection. Therefore, the vulnerabilities of contiguous networks have given reason for many military applications to utilize non-contiguous networks.

Titan Rain was effective if its intent was cyber espionage and bolstering Chinese threat credibility. The attacks seemed to originate from China. Since China is home to millions of unsecured computers, it is conceivable that this attack went through Chinese computers, but actually originated in a different country. However, the investigators of this attack reported that the length and thoroughness of the attack definitely point to Chinese government involvement.[40] Covert remote control of US military networks by an adversary could have many repercussions. For instance, DDoS cyber attacks cutting off US armed forces e-mail and Internet-based lines of communication could severely hamper US armed forces' logistics and supply networks. If the speed and ability of these networks is affected in a negative way, warfighters might not be able to get to the fight, have the right supplies to fight, or get home from the fight effectively and in a timely manner. If the US armed forces cannot perform their missions in a timely manner, strategic opportunities may be lost. Therefore, the threat of an adversary – such as the Chinese – having the ability to hamper the timeliness of US armed forces' is a grave concern.

Conficker

[38] James J. Forest, *Homeland Security: Critical Infrastructure*, (Westport, CT, Greenwood Publishing Group, 2006), 346.
[39] Dawn S. Onley, Patience Wait, "Red Storm Rising," GCN.com, 17 August 2006, http://gcn.com/articles/2006/08/17/red-storm-rising.aspx, (accessed: 28 March 2009).
[40] Forest, *Homeland Security*, 347.

In October 2008, the contagious Conficker worm started residing within the Internet and has been infecting computers ever since. As of March 2009, the Conficker worm infected over ten million computers worldwide. Its main target seems to be corporations.[41] A worm like this undermines common trust in Internet-based applications. The Conficker worm is made up of a sleeper cell of bots, waiting for instructions to engage as a botnet of zombie computers. Conficker.B runs through the Autorun function in Windows and spreads through local area networks and removable storage devices. Conficker.C downloads a Trojan and shuts down security services and blocks connections to security web sites.[42] According to Symantec's website, 500 of the over 50,000 domains infected are due to get an updated copy of the enabling malware of Conficker.[43]

The Conficker worm has Ukrainian origins and its suspected creator is an Eastern European criminal gang with a profit motive.[44] The unknown bot-herder controlling the programs sent out commands.[45] The commands made the botnet connect to other domains infected with the Waledac worm. The Waledac worm sends programs known as "scareware" to personal computers that warn users of an infection. Then, it asks for credit card numbers to pay for bogus antivirus software that infects their computer again.[46] Paul Ferguson, an advanced cyber threats researcher for Trend Micro said recently, "I'm pretty certain the same people are behind both of these worms. Conficker has got their (Waledac creators') fingerprints all over it. There is empirical evidence that these guys are a for-hire, for-profit criminal operation on the Internet and that Conficker is nothing more than part of that organization's best efforts to monetize their efforts on the Internet."[47]

---

[41] Leslie Stahl, "The Conficker Worm: What Happens Next?, 60 Minutes: Computer Worm Could Receive New Instructions On April 1," *60 Minutes, CBS.com*, 29 March 20009, http://www.cbsnews.com/stories/2009/03/27/60minutes/main4897053.shtml, (accessed: 30 March 2009).
[42] BBC News, "Timeline: The Conficker Worm," 31 March 2009, http://news.bbc.co.uk/2/hi/technology/7973829.stm, (accessed: 4 April 2009).
[43] John Markoff, "Worm Infects Millions of Computers Worldwide," *CNET.com*, 22 January 2009, http://www.nytimes.com/2009/01/23/technology/internet/23worm.html?_r=1&em, (accessed: 8 April 2009).
[44] Elinor Mills, "Researchers say Conficker is all about the money," *CNET.com*, http://news.cnet.com/8301-1009_3-10216205-83.html, (accessed: 9 April 2009).
[45] John Markoff, "Worm Infects Millions of Computers Worldwide," *CNET.com*, 22 January 2009, http://www.nytimes.com/2009/01/23/technology/internet/23worm.html?_r=1&em, (accessed: 8 April 2009).
[46] Elinor Mills, "Researchers say Conficker is all about the money," *CNET.com*, http://news.cnet.com/8301-1009_3-10216205-83.html, (accessed: 9 April 2009).
[47] Elinor Mills, "Researchers say Conficker is all about the money," *CNET.com*, http://news.cnet.com/8301-1009_3-10216205-83.html, (accessed: 9 April 2009).

Conficker has undermined common trust in Internet-based applications. It is biding its time, residing within the Internet as a ticking time bomb with an infinite fuse. Conficker has not unleashed any adversarial payload to date and its full effects have yet to be felt.[48] This worm was set to release its unidentified malicious payload as of 1 April 2009. On April fool's day, millions of users braced themselves for Conficker, but nothing happened.[49] Conficker did, however, activate a week later. It directed infected computers to transmit their updates and dropped a mysterious payload. The contents of this payload are still unknown.[50]

Conficker is responsible for crippling military command and control systems. It caused the French Air Force to ground some of its fighter aircraft.[51] It also caused British aircraft and naval vessels' navigation systems not to work properly and has stopped some operations.[52] Effects such as these could impair the deployment of military forces around the world. If a military was hampered in crisis response or wartime operations, endless repercussions and unknown – and possibly unacceptable – consequences could result. If an adversary proves accountable for Conficker, he/she could potentially use Conficker as a coercive instrument. The effectiveness of Conficker to be used as a coercive instrument would depend on the communication of a future Conficker threat, its credibility to inflict future pain, and the commitment of the adversary that chooses to use Conficker to threaten an opponent.

Conclusion

This chapter examined over a decade's worth of cyber attacks against the US. The details of Solar Sunrise, Code Red, Mountain View, Nimda, Slammer, Titan Rain, and Conficker are important to comprehending the coercive effectiveness of cyberpower. None of these attacks held coercive potential since none were accompanied by any

[48] BBC News, "Clock ticking on worm attack code," 20 January 2009, *BBC.com*, *http://news.bbc.co.uk/1/hi/technology/7832652.stm*, (accessed: 12 May 2009).
[49] Justin Ryan, "Conficker Conflunks," *Linux Journal*, 2 April 2009, http://www.linuxjournal.com/content/conficker-conflunks, (accessed: 12 May 2009).
[50] Elinor Mills, "FAQ: Conficker time bomb ticks, but don't expect boom," *CNET com*, 25 March, 2009, http://news.cnet.com/faq-conficker-time-bomb-ticks-but-dont-expect-boom, (accessed: 8 April 2009).
[51] Wright Squawks, "French fighter aircraft grounded by virus attack," 11 February 2009, http://wrightsquawks.blogspot.com/2009/02/french-fighter-aircraft-grounded-by.html, (accessed: 12 May 2009).
[52] Justin Ryan, "Newstradamus Reports: Navy Nailed by Virus," *Linux Journal*, 19 January 2009, http://www.linuxjournal.com/content/newstradamus-reports-navy-nailed-virus, (accessed: 12 May 2009).

communication to the US expressing threats or demands to either divert from the status quo or maintain the status quo. Instead, all of these attacks stemmed from criminal, hacktivist, or espionage-related activities.

These attacks present unknown threats, exploit vulnerabilities, and affect general trust in the US cyber infrastructure. President George W. Bush mentions this in the 2003 US National Strategy to Secure Cyberspace:

> "In the past few years, threats in cyberspace have risen dramatically. The policy of the United States is to protect against the debilitating disruption of the operation of information systems for critical infrastructures and, thereby, help to protect the people, economy, and national security of the United States. We must act to reduce our vulnerabilities to these threats before they can be exploited to damage the cyber systems supporting our Nation's critical infrastructures and ensure that such disruptions of cyberspace are infrequent, of minimal duration, manageable, and cause the least damage possible."[53]

The next chapter parses out the 2007 cyber attacks against Estonia relevant to this study. The biggest differences between the US cases and the attack in Estonia include motive, intent, and organization of the cyber attacks.

[53] The White House, *"The National Strategy to Secure Cyberspace,"* February 2003.

Chapter 3

Web War I in Estonia

The Republic of Estonia is a cyber-dependent nation, making it vulnerable to cyber attacks.[1] This case study focuses on the 2007 cyber attacks on Estonia, referred to as Web War I.

Estonia is wedged between the Baltic Sea and Russia and is slightly smaller than New Hampshire and Vermont combined. About 1.4 million people call Estonia home. In 1940, the USSR claimed sovereignty, but Estonia regained freedom in 1991. Since then, it has sought economic and political ties with Western Europe. It is a member of the United Nations (UN), the North Atlantic Treaty Organization (NATO), and the European Union (EU). Estonia is a parliamentary representative democratic republic.[2]

Cyber-dependent countries like Estonia are vulnerable to cyber warfare. Cyber attacks acts performed against cyber-dependent nations in the last decade have forced countries to reexamine their conceptions of cyber infrastructure security. This security is dependent on the lengths that the nation's enemies are willing to go to. These lengths may include cyber attacks spanning from short-term denial of service attacks to long-term and permanently damaging attacks to the critical pieces of cyber infrastructure. However, due to the ability of cyber infrastructure to be rapidly reconstructed, cyberpower has yet to deliver long-term damaging effects. A range of hackers, both rogue and state-sponsored, can carry out these attacks. The 2007 cyber attacks on Estonia appeared to stem from both types of hacker. Generally, these attacks on Estonia set the precedent for cyber warfare applied against a state.[3]

Estonia may be small, but it has a large number of Internet users per capita compared to most countries. Internet services are widely available to most of the population. By the year 2000, the Estonian government declared Internet access a human

---

[1] Grant, "Victory in Cyberspace," 5.
[2] US Central Intelligence Agency, *The World Factbook, 2008*, https://www.cia.gov/library/publications/the-world-factbook/geos/en.html, (accessed: 28 February 2009).
[3] Stuart Notholt, *Fields of Fire: An Atlas of Ethnic Conflict*, (Kibworth Beauchamp, Leicester, Troubador Publishing Ltd., 2008), 7.07.

right.[4] In 2005 and 2007, Estonia was the first nation in the world to accomplish Internet voting in national elections.[5] Over 90 percent of Estonia is dependent on its cyber infrastructure.[6] All Estonian schools and libraries have Internet access. Estonians file their tax returns, vote, shop, go to school, use Voice Over Internet Protocol (VoIP) communications, and bank online.[7] A wide range of high quality voice, data, and Internet services are available throughout the country.

To facilitate a clear understanding of the cyber attacks in Estonia, and in the next chapter's case study of the cyber attacks in Georgia, this analysis uses a common framework. To organize this analysis we will examine the prominent features of each attack, consisting of background, course of events, objective, and an exacerbating factor. In the Estonian case, the background is full of social tensions stemming from Estonia's independence from the Soviet Union in 1991. The course of the attacks included three short escalating events, lasting not more than a month. Generally, the objective of these cyber attacks seemed to be political. They were directly aimed at the Estonian government and society. Finally, an exacerbating factor making the cyber attacks against Estonia effective stemmed from Estonia's cyber infrastructure being unprepared for all out cyber warfare.

Web War I

The cyber attacks against Estonia started the night of 26 April 2007.[8] Press reports refer to the attacks as, "Web War I."[9] The attacks started after the Estonian government made plans to move a Russian war statue and memorial from the capital city of Tallinn to the suburbs. It was a large, bronze, 6-foot tall, 1947 Soviet-era statue that commemorates the Russian war dead that drove the Nazis out of the Soviet Union in World War II.[10] Soon after the end of WWII, the Russians deported Estonians to Serbia

[4] "Marching Off to Cyberwar," *The Economist Technology Quarterly*, 6 December 2008, 20-21.
[5] "Estonia Pulls Off Nationwide Net Voting," *CNET News*, 19 October 2005, http://news.cnet.com/Estonia-pulls-off-nationwide-Net-voting/2100-1028_3-5898115.html, (accessed: 28 February 2009).
[6] "Marching Off to Cyberwar," *The Economist Technology Quarterly*, 6 December 2008, 20-21.
[7] US Central Intelligence Agency, *The World Factbook, 2008*, https://www.cia.gov/library/publications/the-world-factbook/geos/en.html, (accessed: 28 February 2009).
[8] "A Cyber-riot," *The Economist*, 12 May 2007, Vol. 383 Issue 8528, 55.
[9] Grant, "Victory in Cyberspace," 5.
[10] Steven Lee Myers, "Estonia Computers Blitzed, Possibly by the Russians," *New York Times*, 19 May 2007, http://www.nytimes.com/2007/05/19/world/europe/19russia.html?fta=y (accessed: 1 March 2009).

and forcibly took over Estonia.[11] For that reason, to some ethnic Estonians, this statue represents Russian oppression.[12] When the Russian government learned of the Estonian government's plan to move the statue, they threatened that the removal would be "disastrous for Estonians."[13] Within three days, amidst violent gatherings and protests by ethnic Russians, the government removed the statue from its downtown location and installed it at a military cemetery in the suburbs outside of Tallinn.[14]

Figure 4 Estonia Website Defaced with Picture of a Russian Soldier
"The Cyber Raiders Hitting Estonia," *BBC News*, International Version, 17 May 2007, http://news.bbc.co.uk/2/hi/europe/6665195.stm, (accessed: 28 February 2009).

Figure 5. Hackers Hit Both Ways… A Pro-Statue Website was Hacked to Show Estonia's Flag
The Cyber Raiders Hitting Estonia," *BBC News*, International Version, 17 May 2007, http://news.bbc.co.uk/2/hi/europe/6665195.stm, (accessed: 28 February 2009).

Web War I was coordinated in three stages commencing on 28 April, 4 May, and 9 May 2007.[15] It included tactical script kiddie cyber exploitation; operational rouge botnet (robot network) and zombie attack; and defacement of commercial and

[11] "Hackers Take Down the Most Wired Country in Europe," *Wired Magazine, Issue 15.09*, 21 August 2007, http://www.wired.com/politics/security/magazine/15-09/ff_estonia, (accessed: 28 February 2009).
[12] "Hackers Take Down the Most Wired Country in Europe," *Wired Magazine, Issue 15.09*, 21 August 2007, http://www.wired.com/politics/security/magazine/15-09/ff_estonia, (accessed: 28 February 2009).
[13] "Hackers Take Down the Most Wired Country in Europe," *Wired Magazine, Issue 15.09*, 21 August 2007, http://www.wired.com/politics/security/magazine/15-09/ff_estonia, (accessed: 28 February 2009).
[14] Binoy Kampmark, "Cyber Warfare Between Estonia and Russia," *Contemporary Review*, Autumn 2007: 293.
[15] See Binoy Kampmark, "Cyber Warfare Between Estonia and Russia," *Contemporary Review*, Autumn 2007: 293; "Hackers Take Down the Most Wired Country in Europe," *Wired Magazine, Issue 15.09*, 21 August 2007, http://www.wired.com/politics/security/magazine/15-09/ff_estonia, (accessed: 28 February 2009); and "Marching Off to Cyberwar," *The Economist Technology Quarterly*, 6 December 2008, 20-21.

government websites.[16] "Attacks were carried out by amateurs and by highly skilled cyber attack specialists with significant resources."[17] The "cyber attack specialists with significant resources" could have been state-sponsored hackers.[18] Bursts of electronic messages began to flood government websites and servers. The websites of the Estonian Prime Minister, Parliament, Foreign Ministry, Ministry of Internal Affairs and Ministry of Economic Affairs and Communications all went down.[19] Estonian officials traced the source of the problems and discovered that computers located inside the Russian government were responsible.[20] It was an all out cyber war. Estonian Internet security defenses were completely overwhelmed when the attack count reached over 1,000 assaults on the first day.[21] One effect of these attacks directly affected the parliament's critical communications infrastructure, as the parliament's e-mail server was an early casualty.[22] Attacks grew to over 2,000 *an hour* by the second day.[23] The DDoS attacks forced the government to shut down critical websites. On the third day, 9 May, the attacks peaked.[24] With every second that ticked by, these cyber attacks hit Estonia's cyber infrastructure with an estimated four million packets of data.[25]

According to Jaak Aaviksoo, Estonian Minister of Defense, the main targets of the botnet attacks were major commercial banks, telephone companies, media outlets, and Internet name servers. He said, "This was the first time a botnet threatened the national security of an entire nation. Unlike a nuclear or conventional military attack, you do not need a government for such attacks."[26] He also mentioned that there was a

---

[16] In its simplest form, a botnet is an army of compromised computers that take orders from a botherder. A botherder is a hacker who uses the botnet for financial gain or as a weapon against others, usually via illegal means. See Craig A. Schiller, Jim Binkley, Davis Harley, Gadi Evron, Tony Bradley, *Botnets, the Killer Web App*, (Syngress, 2007), 3.
[17] A bot is an automated program that accesses web sites then transverses the site by following links on its pages; bots typically have some form of artificial intelligence and carry out tasks in lieu of a real person. See Grant, "Victory in Cyberspace," 5.
[18] Grant, "Victory in Cyberspace," 10.
[19] "Hackers Take Down the Most Wired Country in Europe," *Wired Magazine, Issue 15.09,* 21 August 2007, http://www.wired.com/politics/security/magazine/15-09/ff_estonia, (accessed: 28 February 2009).
[20] "Hackers Take Down the Most Wired Country in Europe," *Wired Magazine, Issue 15.09,* 21 August 2007, http://www.wired.com/politics/security/magazine/15-09/ff_estonia, (accessed: 28 February 2009).
[21] Grant, "Victory in Cyberspace," 5.
[22] Steven Lee Myers, "Estonia Computers Blitzed, Possibly by the Russians," *New York Times,* 19 May 2007, http://www.nytimes.com/2007/05/19/world/europe/19russia.html?fta=y (accessed: 1 March 2009).
[23] Grant, "Victory in Cyberspace," 5.
[24] Grant, "Victory in Cyberspace," 5.
[25] Data Packet: A packet is a basic unit of communication over a digital network. A packet is also called a datagram, a segment, a block, a cell or a frame, depending on the protocol. When data has to be transmitted, it is broken down into similar structures of data, which are reassembled to the original data chunk once they reach their destination.
[26] "Hackers Take Down the Most Wired Country in Europe," *Wired Magazine, Issue 15.09,* 21 August 2007, http://www.wired.com/politics/security/magazine/15-09/ff_estonia, (accessed: 28 February 2009).

much more subtle and sophisticated attack against critical infrastructure embedded in the noise of the DDoS attacks. "The computer attacks on Estonia were vectored in from more than 50 countries. Many attacking computers had been co-opted by operators in other countries."[27] The desired effect was to degrade Estonia's Internet connectivity. Before permanent damage occurred to the Estonian cyber infrastructure, Estonian authorities were able to thwart this phase of the attacks.[28]

The botnet and zombie attacks lasted through 9 May 2007. They denied Internet access for the entire country.[29] The botnets and zombies attacked Estonian governmental websites and servers. The attacks rendered Estonian news portals unusable. The attacks also affected the two largest banks in Estonia, shutting down over 90 percent of online banking operations. Affected commercial entities included banks, several Internet Service Providers and telecoms.[30] The hackers implanted zombies into hundreds of thousands of computers, worldwide.[31] Zombies are capable of repeatedly flooding designated Internet addresses with a variety of useless network-clogging data, creating an impassible data debris field.[32] Finally, these offensive cyber attacks included hacktivists that deleted information on commercial and government websites and replaced it with their messages. Some of these messages, posted by a hacker named "S1B," said, "DDoS is occurring even now but something more potent is on its way. :)." S1B went on to say, "On the 9th of May a mass attack is planned…The action will be massive — it's planned to take, Estonnet the $@!# down. :)"

This brand of cyber warfare has far-reaching implications. Several critical pieces of the cyber infrastructure were kicked offline: Estonian government websites and e-mail servers, commercial news outlets (online newspapers), ATM machines, all commercial online banking services, Sykpe (VoIP communications), telephone companies, and name

---

[27] Grant, "Victory in Cyberspace," 5.
[28] "Hackers Take Down the Most Wired Country in Europe," *Wired Magazine, Issue 15.09,* 21 August 2007, http://www.wired.com/politics/security/magazine/15-09/ff_estonia, (accessed: 28 February 2009).
[29] Grant, "Victory in Cyberspace," 4.
[30] A 'bot' is a type of malware that allows an attacker to gain complete control over the affected computer. Bot infected computers are generally referred to as 'zombies'. See About.com: Internet Security, "bots and zombies," http://netsecurity.about.com/od/frequentlyaskedquestions/qt/pr_bot.htm, (accessed: 29 March 2009).
[31] "Hackers Take Down the Most Wired Country in Europe," *Wired Magazine, Issue 15.09,* 21 August 2007, http://www.wired.com/politics/security/magazine/15-09/ff_estonia, (accessed: 28 February 2009).
[32] Craig A. Schiller, Jim Binkley, David Harley, Gadi Evron, Tony Bradley, *Botnets,* (New York: Syngress, 2007), 30-31.

servers.[33] By and large, if all these pieces of infrastructure had continued to be denied, degraded, or destroyed for over 6 months, this could have had a detrimental effect on the Estonian society.[34] The way of life for the Estonian citizen was changed. According to an Estonian Internet expert, "We are back in the stone age, telling the world what is going on with phone and fax."[35] If the effects of the attacks were permanent, the Estonian government would have to pay the costs of restructuring their country's cyber infrastructure to regain Internet access for the Internet-centric country and accept one of two alternatives. The Estonians could accept no Internet connectivity with the rest of the free world and decide to realign their society and culture accordingly; or the government could choose to comply with the coercer's demands of returning the Soviet statue to its original location.

The destructive possibilities of cyber attacks like the ones against Estonia are unknown at this time. DDoS attack is not the most dangerous form of cyber attack. Many networks that experience a DDoS attack are back online as soon as the experts who run them update security software or clean the systems of malware.[36] One of the most dangerous forms of cyber attack consists of malicious code that scrambles or erases data such as bank accounts or health records.[37] This did not happen in Estonia, but the intruders had the access required if they had wanted to spread this type of destructive payload.

Countries that are cyber-dependent can become cyber-locked in the same way that countries are land-locked. Paper-less societies, such as Estonia, can become cyber-locked if their *paper-less* foundation – the command and control of their cyber infrastructure – is taken away. Therefore, attacks such as the ones conducted against Estonia, can *cyber-lock* a country. *Cyber-locked* countries like Estonia might have had to rely too heavily on a handful of cyberspace connections to the outside world, potentially through hostile countries.[38] If this had happened the adversary might have

---

[33] "Hackers Take Down the Most Wired Country in Europe," *Wired Magazine, Issue 15.09,* 21 August 2007, http://www.wired.com/politics/security/magazine/15-09/ff_estonia, (accessed: 28 February 2009).
[34] "A Cyber-riot," *The Economist,* 12 May 2007, Vol. 383 Issue 8528, 55.
[35] "A Cyber-riot," *The Economist,* 12 May 2007, Vol. 383 Issue 8528, 55.
[36] Bidgoli, *Handbook of Information Security*, 96.
[37] Bidgoli, *Handbook of Information Security*, 96.
[38] Centre of Excellence Defence Against Terrorism, N. P., *Responses to Cyber Terrorism,* (New York, NY: IOS Press, 2008). 98.

been able to control the country's entire network access to the outside world. This would have forced Estonian society to restructure itself away from cyber-dependency, depending on the destruction caused to the Estonian cyber infrastructure, economy, and resources available for rebuilding. Hypothetically, Estonia's cyber infrastructure could have been held for ransom.

The fact that Estonian Internet connections were unable to handle large, sustained traffic flows exacerbated the attacks.[39] The Estonian model set a precedent for the type of security other states need to have if they do not want adversaries to exploit similar vulnerabilities. The Sweden Emergency Management Agency published a report in 2008, which studied the Estonia case in detail. Sweden is concerned because it occupies the same geographic region and hosts a large amount of worldwide online banking activity.[40] If their banks were hit as badly as Estonia's were, their financial centers would be affected with unknown repercussions.[41]

The perpetrator of these cyber attacks is still unknown. Despite forensic evidence that the Russian government was involved in these attacks, the Russian government has not assumed responsibility.[42] Even though there is no conclusive evidence that the Russian government sanctioned these attacks, there is also no evidence that it did anything to stop them.[43] Hackers hijacked the Internet sites used in these cyber warfare actions. These sites enabled a proxy war against the Estonian cyber infrastructure. Evidence points to the involvement of some Russian citizens in the following quote from leading Internet Security expert, Gadi Evron[44]:

> "In the days leading up to the attacks, numerous clues pointed to a large-scale operation that was being planned online. Russian language Internet discussion forums were abuzz with preparations for an online attack. Three days before the expected onslaught, Estonia planned to release the news of the coming strike in hopes that European media attention would oblige the EU to pressure

[39] General assumption based on personal discussions with US Chairman of Joint Chiefs of Staff, Joint Staff, Cyberspace Operations and Policy Division Action Officers and Directors, 30 March 2009, Pentagon, Washington, DC.
[40] Swedish Emergency Management Agency (SEMA), *Large Scale Internet Attacks, The Internet Attacks on Estonia*, (Huskvarna, Swedish Emergency Management Agency, 2008), 1-20.
[41] SEMA, *The Internet Attacks on Estonia*, 1-20.
[42] SEMA, *The Internet Attacks on Estonia*, 1-20.
[43] "Marching Off to Cyberwar," *The Economist Technology Quarterly*, 6 December 2008, 20-21.
[44] Gadi Evron is recognized for his work and leadership in Internet security operations and is arguably the world's top expert on botnets. Previously, he was Chief Information Security Officer at the Israeli government Internet Service Provider.

> the Kremlin to intervene…it remains unclear if it was the Russian government, but it is undisputed that Russians were responsible." [45]

Overall, these attacks set the precedent for debilitating cyber attacks on a state. This was the first documented open source case of coercion being attempted using cyberpower. Estonia was unable to utilize its cyber-infrastructure. The daily lives of most Estonians changed due to these attacks.[46] All Internet-based applications and were shutdown and most banking services were unavailable. If these attacks had been longer in duration or more severe in their effects, they could have severely crippled Estonia and induced economic ruin. It is also possible that long-term degradation of the government's ability to command and control of its instruments of power could have put the nation into a position of weakness, making it ripe for takeover by an adversary.[47]

The attacks were short term and Estonia was not alone in the cyber defensive actions it took. NATO took quick notice of Estonia's cyber attacks. NATO's Secretary General Jaap de Hoop Scheffer said, "No member state is protected from cyber attacks."[48] A senior official in Brussels asked, "If a member state's communications centre is attacked with a missile, you can call it an act of war. So what do you call it if the same installation is disabled with a cyber attack?"[49] U.S. Air Force Secretary Michael Wynne was alarmed, "Russia, our Cold War nemesis, seems to have been the first to engage in cyber warfare...these are the first known incidents of such an assault on a state."[50] At the June 2007 NATO meeting, the U.S. Secretary of Defense, Robert Gates, urged defense ministers to think about cyber attack response options.[51]

Estonia took measures with NATO and the UN. Estonia sought to put the issue of cyber attacks on the security-policy agenda. Estonia appealed for a UN convention on cyber warfare and cyber terrorism.[52] Estonia's request for NATO to establish cyber security measures has strategic implications. If cyber attacks were included in NATO's

---

[45] Gadi Evron, "Battling Botnets and Online Mobs - Estonia's Defense Efforts during the Internet War," *Science & Technology*, Winter/Spring 2008.
[46] "Hackers Take Down the Most Wired Country in Europe," *Wired Magazine, Issue 15.09,* 21 August 2007, http://www.wired.com/politics/security/magazine/15-09/ff_estonia, (accessed: 28 February 2009).
[47] This is discussed in detail in chapter four.
[48] Grant, "Victory in Cyberspace," 4.
[49] "A Cyber-riot," *The Economist,* 12 May 2007, Vol. 383 Issue 8528, 55.
[50] Grant, "Victory in Cyberspace," 4.
[51] Greg Jaffe, "Gates Urges NATO Ministers to Defend Against Cyber Attacks," *Wall Street Journal,* 15 June 2007.
[52] SEMA, *The Internet Attacks on Estonia*, 4-20.

security agreements, this would justify other NATO member nations taking action against the perpetrators of cyber attacks. Therefore, NATO member countries could get the same protection and committed defense against possible future cyber attacks.

Estonia requested assistance from the EU. Estonia is the smallest member of the EU. The EU adopted a resolution concerning the cyber attacks on Estonia. Part of this resolution addressed the refusal of the Russian government to cooperate in stopping the cyber attacks.[53] Afterwards, the EU called for a study on "how such attacks and threats can be addressed at the EU level."[54] Since no official Russian entity took responsibility for these attacks, the European Parliament refrained from comment.[55]

Conclusion

This attempt at using cyberpower to coerce failed. The movement of the Russian war memorial to the suburbs outside Tallinn occurred.[56] The coercer did not achieve the intended aim of maintaining the status quo. The Estonian government moved the statue from its original location and established a new status quo. The hackers were likewise unsuccessful in compelling Estonia to return the statue to the middle of Tallinn. Hence, it was a failed attempt at coercion.

The cyber attacks on Estonia proved how vulnerable this cyber-dependent state is to cyber warfare. Estonia has reexamined its conceptions of cyber infrastructure security and has is actions to establish a NATO-sponsored Estonian Cyber Defense center.[57] A range of hackers, both rogue and state-sponsored, appeared to perform these attacks in organized ways. Generally, these attacks on Estonia set the precedent for cyber warfare applied against a state.[58] This was the first time that cyberpower was used as a coercive instrument against a state. Cyberpower in this case did not prove to be effective at coercion.

---

[53] Richard C. Ragaini, R. Ragaini, *International Seminar on Nuclear War and Planetary Emergencies — 38th Session*, (Singapore, World Scientific, 2008), 485.
[54] Richard C. Ragaini, R. Ragaini, *International Seminar on Nuclear War and Planetary Emergencies — 38th Session*, (Singapore, World Scientific, 2008), 485.
[55] Ragaini, *International Seminar on Nuclear War and Planetary Emergencies — 38th Session*, 485.
[56] Grant, "Victory in Cyberspace," 5.
[57] Bruce Sterling, "Estonia: NATO's Brand New Center of Cyberwarfare Excellence," *WIRED.com*, 30 April 2008, http://www.wired.com/beyond_the_beyond/2008/04/estonia-natos-b/, (accessed: 4 June 2009).
[58] Stuart Notholt, *Fields of Fire: An Atlas of Ethnic Conflict*, (Kibworth Beauchamp, Leicester, Troubador Publishing Ltd., 2008), 7.07.

In comparison with the cyber attacks on the US, the attacks on Estonia seemed to have motive, intent, and organization. Because of Estonia's small size, these attacks held more affect against the state. In the chapter that follows, cyber warfare takes a step further and is combined with physical force.

Chapter 4

Cyber Attack on Georgia

> *In the very near future many conflicts will not take place on the open field of battle, but rather in spaces on the Internet, fought with the aid of information soldiers, that is hackers. This means that a small force of hackers is stronger than the multi-thousand force of the current armed forces.*
>
> —Nikolai Kuryanovich
> Deputy of the Liberal and Democratic Party of Russia

The Republic of Georgia is a small independent state. Its growing cyber-dependence makes it vulnerable to cyber attack. Georgia is a state wrought with social tensions stemming from ethnic minority groups wanting independence from Georgia.[1] Ethnic minority groups in South Ossetia and Abkhazia want independence from Georgian governance. These groups want the Georgian government to see them as independent states with the right to determine their own future.[2] This final case study focuses on the July-August 2008 cyber attacks on Georgia, as part of the 2008 South Ossetia War.

To facilitate a clear understanding of the cyber attacks in Georgia, this analysis uses the same framework as in chapters two and three. To organize this analysis the background, course of events, and Russian objective of these attacks are examined. First, social tension in Georgia stems from past Russian aggression in the regions of Abkhazia and South Ossetia. Second, these cyber attacks occurred from mid July – mid August 2008 and effectively shut down the cyber infrastructure of Georgia. These events started before and continued throughout the Russian and Georgian ground and air campaigns. Third, the likely operational objective of this cyber warfare campaign was to facilitate the Russian invasion and occupation of Abkhazia and South Ossetia. Russian actions illustrated two strategic aims. Number one, the Russians wished to keep Georgia from attaining NATO membership.[3] Number two, the Russians wanted Georgia to give full

[1] Jim Nichol, CRS Report for Congress, "Russia-Georgia Conflict in South Ossetia: Context and Implications for U.S. Interests," September 22, 2008 (US Congress, Washington DC, 2008), 1-10.
[2] Nichol, CRS Report for Congress, "Russia-Georgia Conflict in South Ossetia," 1-10.
[3] Nichol, CRS Report for Congress, "Russia-Georgia Conflict in South Ossetia," 20-29.

independence to the regions of Abkhazia and South Ossetia.[4] Finally, the small size of the Georgian cyber infrastructure made it easy to overtake and shutdown.

Georgia is vulnerable to cyber and physical attacks for many reasons. These include a struggling democratic government, a strategic geographic location, and ethnic minority conflicts. Georgia has come a long way since gaining independence in 1991 from the Soviet Union. Georgia has a population of about 1.4 million people and is a parliamentary representative democratic republic.[5] Geographically, Georgia is slightly smaller than North Carolina and it is strategically located east of the Black Sea, south of Russia. This location enables it to control the lines of communication through the Caucasus Mountains. Running through the mountains from Azerbaijan is a US-backed oil pipeline. "The US backed the Baku-Tblilisi-Ceyhan (BTC) pipeline, connecting the Caspian Sea to the Mediterranean, to diversify the export routes of Caspian oil, and to increase export volumes by adding pipeline capacity and encouraging foreign investment in Kazakhstan and Azerbaijan."[6] According to Richard Sokolsky, et al., in their book *Persian Gulf Security,* "Any Azeri oil… headed west toward the Mediterranean would be vulnerable to secessionist struggles in Georgia."[7] This oil pipeline allows the West to reduce its reliance on Middle Eastern oil while bypassing Russia and Iran.[8]

The largest challenges for Georgian growth are the ethnic minority conflicts in the Russian-backed breakaway regions of Abkhazia (in western Georgia) and South Ossetia (in northern Georgia).[9] Tensions between Georgia and Russia date back to at least the 1920's.[10] In 1991, over 10,000 people were displaced and almost 4,000 deaths occurred during an ethnic Georgian-South Ossetian conflict. In 1992, Russia brokered a cease-fire and Russian, Ossetian, and Georgian forces set up "peacekeeping" forces in the region.[11] After the end of the South Ossetian war in 1992, a joint Russian-Georgian peacekeeping

---

[4] Nichol, CRS Report for Congress, "Russia-Georgia Conflict in South Ossetia," 20-29.
[5] US Central Intelligence Agency, *The World Factbook, 2008,* https://www.cia.gov/library/publications/the-world-factbook/geos/gg.html, (accessed: 1 March 2009).
[6] Daniel Moran and James A. Russell, *Energy and Global Politics,* (London, UK, Taylor and Francis, 2008), 119.
[7] Richard Sokolsky, Stuart E. Johnson, F. Stephen Larrabee, *Persian Gulf Security: Improving Allied Military Contributions,* (Arlington, VA, RAND Corporation, Project Air Force, 2000), 20.
[8] Anne Gearan, "Georgia's oil pipeline is key to US support," *San Francisco Chronicle.com,* 9 August 2008, http://www.sfgate.com/sports/preps/, (accessed: 7 May 2009).
[9] Resolution of the Parliament of Georgia on the Occupation of the Georgian Territories by the Russian Federation, http://www.parliament.ge/index.php?lang_id=ENG&sec_id=98&info_id=20047, (accessed: 1 March 2009).
[10] Nichol, CRS Report for Congress, "Russia-Georgia Conflict in South Ossetia," Summary.
[11] Nichol, CRS Report for Congress, "Russia-Georgia Conflict in South Ossetia," 1.

force occupied a newly divided South Ossetia. From 1991-1993, a similar conflict over ethnic cleansing was fought in the Abkhazia region.[12]

Russian motivation to conduct cyber and physical attacks against Georgia might stem from the 2003 "Rose Revolution," which brought President Mikheil Saakashvili to power.[13] His administration threatens Russia as it pursues economic and democratic reforms.[14] President Saakashvili has pledged to regain Georgian control over the separatist regions of South Ossetia and Abkhazia, and has tightened border controls, strengthened police forces, and driven out corruption and smuggling operations.[15] In 2005, the South Ossetian government rejected a peace plan announced by President Saakashvili.[16] In late summer of 2008, the Abkhazia militia was encouraged by the Russian expulsion of ethnic Georgians from South Ossetia and Abkhazia.[17] On 7-8 August 2008, Georgian military forces launched a major attack on South Ossetia. The Georgian government aimed to re-take this region as quickly as possible. The Georgian military started its actions by forcefully entering the South Ossetian capital of Tskhinvali.[18] As of 26 August 2008, Russia officially acknowledged South Ossetia and Abkhazia as independent states.[19] The US, France, and Britain do not acknowledge this independence. The only countries that acknowledge South Ossetian and Abkhazian independence are Russia and Nicaragua.[20] This unrest seems to be the root cause of the 2008 cyber and physical attacks on Georgia.

South Ossetia (and Abkhazia) Cyber War of 2008

Starting on 19 July 2008, the Georgian cyber infrastructure experienced overwhelming attacks. Multiple Georgian websites experienced defacement and denial

[12] Ethnic Georgians make up over 47% of the population in this region.
[13] Nichol, CRS Report for Congress, "Russia-Georgia Conflict in South Ossetia," 20-25.
[14] Nichol, CRS Report for Congress, "Russia-Georgia Conflict in South Ossetia," 2.
[15] Nichol, CRS Report for Congress, "Russia-Georgia Conflict in South Ossetia," 2-3.
[16] Nichol, CRS Report for Congress, "Russia-Georgia Conflict in South Ossetia," 1-10.
[17] Nichol, CRS Report for Congress, "Russia-Georgia Conflict in South Ossetia," 2-7.
[18] Matthew Clements, "Georgia Launches Major Assault on South Ossetia," *Janes.com,* 8 August 2008, http://www.janes.com/media/releases/pc080808_2.shtml, (accessed: 24 May 2009).
[19] Sebastian Alison and Lyubov Pronina, "Russia Recognizes Independence of Georgian Regions," *Bloomberg.com,* http://www.bloomberg.com/apps/news?pid=20601082&sid=afAvlgTbOoAg&refer=canada, (accessed: 11 April 2009).
[20] Reuters, "FACTBOX-Key Facts on Rebel Region of South Ossetia," *Reuters.com,* 31 May 2009, http://www.reuters.com/article/asiaCrisis/idUSLV15723, (accessed: 31 May 2009).

of service attacks throughout July and August 2008.[21] Affected Georgian government and news websites included: President Saakashvili's website (www.president.gov.ge); the Parliament's website (www.parliament.ge); general news websites (news.ge, newsgeorgia.ru, and newstula.info); and political news websites (apsny.ge, tbilisiweb.info, os-inform.com, www.kasparov.ru, hacking.ge, mk.ru, skandaly.ru).[22] Other websites included: "The Georgian Hacking Community" (hacking.ge); "skandaly.ru", a Russian scandal blog site; "mk.ru", a Russian classifieds blog and news site; and "www.kasparov.ru", a Russian political activist site. Of note in these lists is the ".ge" for Georgia and ".ru" for Russian sites.[23]

On 8 August 2008, the day after Georgian and Russian troops moved into South Ossetia, there was a noted increase of cyber attacks.[24] By 10 August 2008, the majority of Georgian government websites and e-mail servers were defunct.[25] Georgia was cyberlocked. In the same way a landlocked country has no access to the sea, a cyberlocked country has no access to cyberspace. When a country relies too heavily on a handful of cyberspace connections – potentially through hostile countries for physical connectivity – it is vulnerable to becoming cyberlocked. It follows that if an adversary cuts off the country's cyberspace connections that adversary can effectively cyberlock the country.[26] The Georgian government found work-arounds to these attacks by relocating critical official Internet-based assets to the US, Estonia, and Poland.[27]

Another factor of the cyber attacks on Georgia was the small size of Georgia's cyber infrastructure (relative to those of the US or Estonia). Georgia may have over three times the population of Estonia, but it only has one-sixth the number of Internet hosts and less than half the number of users.[28] Georgia's population of just over 4.6 million

---

[21] Dancho Danchev, "Georgia President's web site under DDoS Attack from Russian hackers," *zdnet.com*, 22 July 2008, http://blogs.zdnet.com/security/?p=1533, (accessed: 21 April 2009).
[22] Steven Adair, "Georgian Websites Under Attack - DDoS and Defacement," *Shadowserver*, 11 August 2008, http://www.shadowserver.org/wiki/pmwiki.php?n=Calendar.20080811, (accessed: 4 March 2009).
[23] Gary Kasparov's website holds the name of "The Other Russia, News from the Coalition for Democracy in Russia."
[24] Stephen W. Korns and Joshua E. Kastenburg, "Georgia's Cyber Left Hook," *Parameters*, Winter 2008-09, 60-75.
[25] Korns and Kastenburg, "Georgia's Cyber Left Hook," *Parameters*.
[26] Centre of Excellence Defence Against Terrorism, N. P., *Responses to Cyber Terrorism*, (New York, NY, IOS Press, 2008). 98.
[27] Korns and Kastenburg, "Georgia's Cyber Left Hook," *Parameters*.
[28] US Central Intelligence Agency, *The World Factbook, 2008*, *https://www.cia.gov/library/publications/the-world-factbook/geos/gg.html*, (accessed: 1 March 2009).

accounts for only one percent of the Internet users in the world.[29] Since Georgia's cyber infrastructure is small, it is easier to attack. With only six Internet service providers, if an aggressor can overpower those six they can take down Georgia's cyber infrastructure foundation. In comparison, the US has over 7,000 Internet service providers (ISPs) and Estonia has 38. Accordingly, effective cyber attacks seem more difficult to accomplish in countries with more ISPs.[30]

In late August 2008, the Georgian government launched an Open Source Intelligence (OSINT) initiative to examine the cyber attacks on the Georgian cyber infrastructure.[31] A US-based cyber investigation firm, named GreyLogic, performed the OSINT. GreyLogic provides services that specifically track non-state hackers for governments and GreyLogic has applied for non-profit status within the US.[32] The OSINT resulted in two reports. The first report, named Project Grey Goose: Phase I, was released 17 October 2008.[33] The second report, named Grey Goose: Phase II, was released 20 March 2009.[34] The Phase I report found the source of the attacks to be two patriotic Russian hacker websites, "www.stopgeorgia.ru" and www.xakep.ru.[35] These patriotic hackers – sometimes referred to as "hacktivists"[36] – use a journeyman-apprentice approach that trains other hackers to do their dirty work. The report concluded that the cyber attacks were part of a premeditated denial of service plan to affect the entire Georgian cyber infrastructure.[37] The follow-up Phase II report included additional findings. It states, "In the case of possible Russian government involvement

---

[29] CIA, *The World Factbook*, https://www.cia.gov/library/publications/the-world-factbook/print/en.html (accessed: 2 May 2009).
[30] CIA, *The World Factbook*, https://www.cia.gov/library/publications/the-world-factbook/print/en.html (accessed: 2 May 2009).
[31] Project Grey Goose Report: Phase I, 17 October 2008, http://www.scribd.com/doc/6967393/Project-Grey-Goose-Phase-I-Report#document_metadata, (accessed: 4 March 2009).
[32] For more information on GreyLogic see http://greylogic.us/
[33] Project Grey Goose Report: Phase I, 17 October 2008, http://www.scribd.com/doc/6967393/Project-Grey-Goose-Phase-I-Report#document_metadata, (accessed: 4 March 2009).
[34] Grey Goose Report: Phase II Report, 20 March 2009, http://greylogic.us/?page_id=85, (accessed: 24 May 2009).
[35] Project Grey Goose is, in technology terms, a pure play Open Source Intelligence (OSINT) initiative launched on August 22, 2008 to examine how the Russian cyber war was conducted against Georgian Web sites and if the Russian government was involved or if it was entirely a grass roots movement by patriotic Russian hackers.
[36] According to Joshua Davis, of Wired Online Magazine, "There is a specific department within the FSB — the internal counterintelligence agency of the Russian Federation and successor to the Soviet KGB; formerly led by Vladimir Putin — that specializes in coordinating Internet campaigns against those they consider a threat. In the past, they attacked Chechen rebel websites and now it appears they have attacked Estonia."[36] Hacktivists need very little money to perform attacks such as this one. Servers with high bandwidth can be rented cheaply in countries as diverse as the US and South Korea.
[37] Project Grey Goose Report: Phase I, 17 October 2008, http://www.scribd.com/doc/6967393/Project-Grey-Goose-Phase-I-Report#document_metadata, (accessed: 4 March 2009).

with the cyber attacks on Georgian government websites in July and August, 2008, the available evidence supports a strong likelihood of GRU/FSB planning and direction at a high level while relying on Nashi intermediaries and the phenomenon of crowd sourcing to obfuscate their involvement and implement their strategy."[38] Nashi is the name for a growing Russian political youth movement affiliated with Prime Minister Vladimir Putin, and is headquartered in Moscow.[39] The attacker's plan included five main components: 1) distribute a static list of targets; 2) engage the average ethnic Russian internet users and empower them with easy to use DDoS tools; 3) distribute lists of remotely structured query language (SQL) injectable to Georgian websites; 4) abuse public lists of email addresses of Georgian politicians; and 5) destroy the Georgian ability to communicate via usual channels.[40]

The Grey Goose reports parsed out this new type of cyber warfare. The reports discovered that four methods of cyber attacks were combined during these attacks: 1) no centralized cyber attack coordination; 2) reduced likelihood of hacker traceability; 3) free and dispersed army of smart users provided via the Russian populace and the ethnic Russians living in Georgia; and 4) general e-mail spam and targeted attacks via botnets.[41] Below is an excerpt from one of the hacktivist's attack messages:

> "We - the representatives of Russian hako-underground, will not tolerate provocation by the Georgian in all its manifestations. We want to live in a free world, but exist in a free-aggression and lies Setevom space. We do not need the guidance from the authorities or other persons, and operates in accordance with their beliefs based on patriotism, conscience, and belief. You can call us criminals and cyber-terrorists, razvyazyvaya with war and killing people. But we will fight and unacceptable aggression against Russia in Space Network. We demand the cessation of attacks on information and government resources Runeta, as well as appeal to all media and journalists with a request to cover events objectively. Until the situation has changed, we will attack the Georgian government and information resources. Do not we have launched an information war; we are not responsible for its consequences. We call for the assistance of all who care about the lies of

[38] GRU stands for Chief Intelligence Directorate of the Soviet General Staff. FSB stands for Former Soviet Bloc. See Grey Goose Report: Phase II Report, 20 March 2009, http://greylogic.us/?page_id=85, (accessed: 24 May 2009).
[39] For further details on Nashi, see Edward Lucas, The New Cold War: Putin's Russia and the Threat to the West (New York: Palgrave Macmillan, 2008), 78-79.
[40] Dancho Danchev, "Georgia President's Web Site Under DDoS Attack from Russian Hackers," *ZDNet*, http://blogs.zdnet.com/security/?p=1533&tag=rbxccnbzd1, (accessed: 1 March 2009).
[41] Project Grey Goose Report: Phase I, 17 October 2008, http://www.scribd.com/doc/6967393/Project-Grey-Goose-Phase-I-Report#document_metadata, (accessed: 4 March 2009) and Grey Goose Report: Phase II Report, 20 March 2009, http://greylogic.us/?page_id=85, (accessed: 24 May 2009).

> Georgian political sites, everyone who is able to inhibit the spread of black information. There is one formal mirror project – www.stopgeorgia.info. All other resources have nothing to do with the movement StopGeorgia.ru."[42]

This new type of cyber warfare can attack prominent websites at will. This attack seemed to be only aimed at websites. If and when adversaries like these attack critical command and control pieces of a country's cyber infrastructure, the results could include a myriad of destructive possibilities.[43]

Whoever defaced President Saakashvili's web site was quite competent. The script kiddies[44] involved in these attacks comprehended the possible psychological impacts of a slideshow portraying Saakashvili as Hitler (Figure 6).[45] If Russian intelligence agency involvement could be proven, this would imply that the Russians would knowingly be involved.

In the cyber attacks on Georgia, it seems that the script kiddies involved thought they were just conducting a cyber-riot *per se,* not a coordinated attack against the cyber infrastructure of the Georgian government for the purpose of facilitating kinetic Russian attacks.[46] In essence, the script kiddies acted as the grunts in a war that they did not know they were fighting. They may or may not have known that their actions were being conglomerated into a coordinated and premeditated cyber campaign to shut down the Georgian cyber infrastructure. They were not part of a formal uniformed armed service

---

[42] Dancho Danchev, "Georgia President's Web Site Under DDoS Attack from Russian Hackers," *ZDNet,* http://blogs.zdnet.com/security/?p=1533&tag=rbxccnbzd1, (accessed: 1 March 2009).

[43] These results and implications are discussed in detail within chapter five.

[44] The pejorative term *script kiddie* refers to someone who does not necessarily understand the tools being used, or the logic behind them – instead the script kiddie simply wants to cause as much damage as possible. Think of a script kiddie as someone who likes to graffiti buildings; the primary goal is defacement, not theft or information gathering. See Allan Liska, *The Practice of Network Security,* (Upper Saddle River, NJ, Prentice Hall PTR, 2003), 42.

[45] The train of logic is easy to follow from the Rose Revolution. The 2005 election of Georgian President Edvard Shevardnadze appeared to be fixed. Soon after this election, mass protests broke out within Georgia. These protests forced the ousting of President Shevardnadze. Subsequently, President Mikhail Saakashvili, the political leader who did win the popular vote, replaced him. Since then, ethnic Russians and Russian intelligence agencies have incessantly sought ways to discredit President Saakashvili. The political end goal of reducing President Saakashvili's credibility included reducing public support for an independent Georgia. In turn, this would help to ensure minimum resistance to Russian occupation of the regions of Abkhazia and South Ossetia.

[46] This is the author's personal conclusion based on the compilation of three sources: Dancho Danchev, "Georgia President's Web Site Under DDoS Attack from Russian Hackers," *ZDNet,* http://blogs.zdnet.com/security/?p=1533&tag=rbxccnbzd1, (accessed: 1 March 2009); Project Grey Goose Report: Phase I, 17 October 2008, http://www.scribd.com/doc/6967393/Project-Grey-Goose-Phase-I-Report#document_metadata, (accessed: 4 March 2009); and Jim Nichol, CRS Report for Congress, "Russia-Georgia Conflict in South Ossetia: Context and Implications for U.S. Interests," September 22, 2008 (US Congress, Washington DC, 2008).

or expert cyber corps. Instead, these were unwitting rogue hackers able to accomplish singular tasks in their homes, at Internet cafés, or anywhere they could find an open Internet portal. Intelligence agencies sometimes use script kiddies of this sort to "risk forward" the responsibility of the cyber attacks.[47] The *risk* of action is forwarded onto the script kiddie versus the intelligence agency or the sponsoring government. This is performed via websites using publicly obtainable DDoS attack tools. Intelligence agencies can coordinate the actions of thousands of rogue hackers, depending on the instructions they post.[48] In simple terms, this is how a proxy cyber war is conducted. This appears to be the type of cyber attacks the Georgian cyber infrastructure experienced.[49]

Figure 6. President Saakashvili's Defaced Website
Picture provided by "Coordinated Russian vs Georgia Cyber Attack in Progress," *ZDNet,* http://blogs.zdnet.com/security/?p=1670. (accessed: 4 March 2009).

[47] Dancho Danchev, "Georgia President's Web Site Under DDoS Attack from Russian Hackers," *ZDNet,* http://blogs.zdnet.com/security/?p=1533&tag=rbxccnbzd1, (accessed: 1 March 2009).
[48] Dancho Danchev, "Georgia President's Web Site Under DDoS Attack from Russian Hackers," *ZDNet,* http://blogs.zdnet.com/security/?p=1533&tag=rbxccnbzd1, (accessed: 1 March 2009).
[49] An abbreviated vignette explains how a proxy cyber war is conducted in detail is parsed out at the end of chapter 5.

The Russian government historically distances itself from the patriotic Russian hacker community, yet provides passive support.[50] The Russian government therefore enjoys plausible deniability, but reaps the strategic benefits from cyber attacks against other states and non-state actors.[51]

The likely operational objective of the cyber attacks was to weaken the Georgian government in order to facilitate a subsequent Russian invasion. These attacks seemed to assist the Russian effort to invade and occupy the Georgian regions of South Ossetia and Abkhazia. In late July 2008, both Georgian and Russian forces conducted military exercises in South Ossetia, which seem to have been a drill for what was to come.[52] The physical attacks by the Russian armed forces against Georgia started on 7 August and lasted through 13 August 2008. These attacks forced the relocation of over 100,000 Georgians.[53] Due to the Russian attacks, the Georgian government complied with Russian wishes and unwillingly ceded the territories of South Ossetia and Abkhazia.[54] As of May 2009, the Republic of Georgia does not recognize the independence of these separatist regions, as they ceded these regions under duress. NATO, the EU, the G7,[55] the US, and the Ukraine consider Russian actions in this case to be a violation of Georgian territorial integrity.[56]

Russia's implied strategic aims for the 2008 cyber and physical attacks on Georgia were: 1) undermine Georgian government legitimacy and economic security, 2) keep Georgia out of NATO, and 3) separate the South Ossetia and Abkhazia regions from Georgian governance.[57] According to Igor Torbakov of The Jamestown Foundation,

---

[50] Project Grey Goose Report: Phase I, 17 October 2008, http://www.scribd.com/doc/6967393/Project-Grey-Goose-Phase-I-Report#document_metadata, (accessed: 4 March 2009).
[51] Project Grey Goose Report: Phase I, 17 October 2008, http://www.scribd.com/doc/6967393/Project-Grey-Goose-Phase-I-Report#document_metadata, (accessed: 4 March 2009).
[52] Nichol, CRS Report for Congress, "Russia-Georgia Conflict in South Ossetia," 1-10.
[53] BBC News, "West Condemns Russia Over Georgia," *BBC news.com*, 26 August 2008, http://news.bbc.co.uk/2/hi/europe/7583164.stm, (accessed: 21 April 2009).
[54] BBC News, "Georgia and Russia Agree on Truce," *BBC news.com*, 13 August 2008, http://news.bbc.co.uk/2/hi/europe/7557457.stm, (accessed: 21 April 2009).
[55] The G7 (also known as the G-7 G-8, or HALEY GROUP) is the meeting of the finance ministers from a group of seven industrialized nations. It was founded in 1976 and now includes Canada, France, Germany, Italy, Japan the United Kingdom, and the United States. See the G7/8 Official Website, http://www.g7.utoronto.ca/finance/index.htm (accessed: 31 May 2009).
[56] BBC News, "West Condemns Russia Over Georgia," *BBC news.com*, 26 August 2008, http://news.bbc.co.uk/2/hi/europe/7583164.stm, (accessed: 21 April 2009).
[57] Igor Torbakov, "The Georgia Crisis and Russia-Turkey Relations," *The Jamestown Foundation*, http://www.jamestown.org/programs/recentreports/single/?tx_ttnews%5Btt_news%5D=34181&tx_ttnews%5BbackPid%5D=7&cHash=12982f773b (accessed: 4 March 2009).

Russia's political goal behind coordinating coercive cyber and physical attacks was to convince NATO against beginning a membership action plan for the Republic of Georgia at the December 2008 or April 2009 NATO meetings.[58] Russia seeks to prevent successful Western-oriented democracies on its border, and it used the war to undermine Georgia's economy.[59] The September 2008 US Congressional Research Service Report on the Context and Implications of the Russia-Georgia conflict states, "On August 12, Russian President Dmitry Medvedev declared that 'the aim of Russia's operation for coercing the Georgian side to peace has been achieved. The aggressor has been punished."[60]

After the events of 7-8 August 2008, delegates at both the UN Security Council and NATO met to draft a resolution for peace in the Caucasus region.[61] Russia and China, however, refused to agree to the UN resolutions proposed by the US, Britain, and France. NATO did not pass a resolution and instead decided on an alternative course of action. At the April 2008 summit, NATO failed to offer the Republic of Georgia a Membership Action Plan (MAP).[62] Even though NATO Secretary General Jaap de Hoop Scheffer still termed Georgia a "highly respected partner of NATO," and said that, "Georgia's hope for a MAP is still very much alive,"[63] there was hesitancy among some NATO members about Georgia's chances for NATO membership.[64] At the December 2008 meeting, NATO members citied "both the higher level of tensions over the separatist regions, Georgia's military incursion into South Ossetia, and the danger of war with Russia" as reasons for their hesitancy to support Georgian entrance into NATO.[65]

Conclusion

This chapter detailed the facts surrounding the cyber attacks on the Republic of Georgia's cyber infrastructure during July-August 2008. The attacks appeared to be

[58] Igor Torbakov, "The Georgia Crisis and Russia-Turkey Relations," *The Jamestown Foundation*, http://www.jamestown.org/programs/recentreports/single/?tx_ttnews%5Btt_news%5D=34181&tx_ttnews%5BbackPid%5D=7&cHash=12982f773b (accessed: 4 March 2009).
[59] See chapter five for an in-depth discussion concerning this topic.
[60] Nichol, CRS Report for Congress, "Russia-Georgia Conflict in South Ossetia," 1.
[61] Nichol, CRS Report for Congress, "Russia-Georgia Conflict in South Ossetia," 1-30.
[62] Rebecca Grant, "Victory in Cyberspace," (Air Force Association Special Report, 2007), 5.
[63] Nichol, CRS Report for Congress, "Russia-Georgia Conflict in South Ossetia," 1-30.
[64] Nichol, CRS Report for Congress, "Russia-Georgia Conflict in South Ossetia," 1-30.
[65] Nichol, CRS Report for Congress, "Russia-Georgia Conflict in South Ossetia," 27-30.

coordinated and synchronized with the actions of Russian military forces as part of a premeditated, military campaign. These attacks were full-scale offensive cyber attacks. They included the script kiddie, the dedicated hacktivist, and possibly Russian intelligence expert cyber-operatives. They denied, degraded, defaced, disrupted, corrupted, or crashed all Georgian government websites, Internet, and e-mail server based communications. The attacks shut down the Georgian cyber infrastructure, undermined the government's capability to provide Internet security, and denied the Internet to Georgian users across the country. However, the cyber attacks were unsuccessful at discrediting or removing President Saakashvili and his administration, who remain in power. Hence, the actions of the cyber attacks against Georgian cyber infrastructure are a mixed result for cyberpower's overall effectiveness in this case.

This case took another step forward in cyber warfare. It combined cyber and physical attacks into an integrated and successful campaign. The next and final chapter of this thesis analyzes cyber as a coercive instrument in relation to the cases presented.

Chapter 5

Coercion via Cyberpower

> *Although attacks in the cybersphere do not involve use of physical weapons, their destructive impacts, physical and otherwise, may be no less lethal to societies.*
>
> *–Jeffrey R. Cooper*

This chapter evaluates the case studies in terms of the coercion theory explained in chapter one and provides conclusions about cyberpower as a coercive instrument. Cyberpower failed to coerce in the cases examined for this study. Although the US cases did not exemplify coercion, they suggest that cyberpower may hold great potential as a future coercive instrument of power. Coercion via cyberpower was also unsuccessful in Estonia. Nevertheless, this case set a precedent of cyber attacks against a country. Georgia's case also set a precedent with simultaneous cyber and physical attacks against a state. However, cyberpower's contribution in the Georgia case remains unclear. Although it shows potential, cyberpower still has shortcomings as a coercive instrument. Shortcomings of using cyberpower to coerce include the challenges associated with establishing threat credibility in cyberspace, the ease of producing countermeasures, and the political and economic implications of its use. Cyberpower could have great impact when used against cyber-dependent targets, such as Information-based countries. It can carry unintended and possibly unacceptable consequences if public-use systems are shut down, maliciously manipulated, or controlled by adversaries.

In the cases studied, deterrence and compellence failed because cyber attacks did not inflict enough punishment to make the threats of cyber attack credible. There was no proof that a threat of cyber attack deterred a target from action in the case studies. There was similarly no proof that the threat of continued cyber attacks induced a target to comply with a coercer's wishes in the cases studied.

In the cases examined, cyberpower used as brute force was successful in denying, disrupting, taking, exploiting, gathering, corrupting, and destroying data and information. Many of the cyber attacks studied effectively denied or disrupted the proper operation of targeted cyber infrastructures. Cyber attack was used to directly achieve objectives

without attempting to convince an adversary to comply with demands. However, these cases did not prove that these brute force cyber attacks by themselves actually changed the target's long-term actions. Brute force actions did not have the desired strategic effects.

US Cases

The US cases are worth considering for what they say about American susceptibility to cyber attack. The field of available large-scale cyber attacks to study is small. These large-scale cases were important to examine and nevertheless yielded valuable information about cyberpower's ability to inflict punishment. The US cases show the potential for cyberpower to inflict punishment in coercive actions. The attackers in these cases were effective at anonymously gathering, exploiting, destroying, and corrupting computer-based data. If cyberpower could hurt a cyber-dependent country like the US badly enough, coercion theory suggests that a country might submit to a coercer's demands. For example, one way a cyberpower can have such an affect is via cyber attacks on a country's financial sector. One such attack was the Nimda worm that attacked the US financial sector.

The Nimda worm might have been intended to undermine US economic credibility and banking security. The US financial sector is a critical hub for the world's economies. If the New York Stock exchange's networks stopped functioning properly due to cyber attack, other worldwide exchanges would feel the blow. Important to note, in cyberspace an adversary could hit a nation's entire financial sector much quicker and with less physical destruction than doing the same thing via kinetic means. Most nation's financial structures are very diverse, so to hit each part with a bomb would be quite time consuming and difficult.[1] A physical attack would require a physical presence. On the other hand, remotely operated cyber attacks do not require a physical presence.

The question should not be whether an adversary is going to launch a punishing cyber attack against the US, but when. In 1996, Presidential Clinton established the Commission on Critical Infrastructure Protection. It was tasked to report the threat on US computer networks, specifically critical telecommunications, oil and gas, electricity,

[1] Verton, *Black Ice*, 163.

bank and financial, transportation, water supply, emergency, and government systems. The commission's charter states how interdependent these systems have become in the US and how much the US has grown dependent upon them.[2] The Defense Science Board also reported on the vulnerability of America's information-based economy to attack:

> "The objective of warfare against agriculturally-based societies was to gain control over their principal source of wealth: land…The objective of war waged against industrially-based societies was to gain control over their principal source of all wealth: the means of production. The objective of warfare to be waged against information-based societies is to gain control over the principal means for sustenance of all wealth: the capacity for coordination of socio-economic dependencies. Military campaigns will be organized to cripple the capacity of an information-based society to carry out its information-dependent enterprises."[3]

The point here is that because societies are information-based, information is now their source of power. So, since America is information-based, it can expect to be attacked at the means of its information power – its critical cyber infrastructure.

All of the US cases seemed to be "proof of concept" or "zero-day exploit" attacks.[4] They tested methods of computer network attack. Based upon the attacks studied here, it appears that none achieved any objectives past causing short-term denial, destruction, corruption, or exploitation of information. What remains unknown is if these attacks were just tests or actually failed attempts to destroy US cyber infrastructure, but the likelihood that the perpetrators were honing their abilities in preparation for future attacks must be seriously considered.

The cyber attacks on the US are not examples of coercion as explained in chapter one because they provide little evidence of cyberpower's ability to coerce. The attackers did not communicate clear threats nor state a clear objective. Consequently, the intent of these attacks remains unknown, there were no threats presented, and no long-term strategic effects were evident. The use of cyberpower did not prove effective as a coercive instrument in these cases. Deterrence and compellence include the communication of a threat. Since there was no clear threat communicated, none of these

[2] Verton, *Black Ice*, 179-181.
[3] Verton, *Black Ice*, 182.
[4] Brian T. Contos, *Enemy at the water cooler,* (Elsevier, St Louis, MO, 2006), 44.

cyber attacks appear to be attempts at coercion. The US did not change its general behavior or actions because of these attacks. No clear evidence of coercion presented itself and it remains unclear what these attacks were intended to accomplish.

The US cases may be examples of foreign entities honing and demonstrating their cyber capabilities in preparation for future coercive acts involving the use of cyberpower. The attacks on the US advertized enemy capabilities. These attacks show that cyberpower is successful at exploiting and gathering information at will. Without testing cyber attack methods, no cyber operator can explore possible coercive benefits. Throughout history, wars have been the proving ground for new technology. In this way, cyber attacks are no different than any other form of warfare.[5] Other forms require adequate real world testing before being considered valid, hence the reasoning behind military wargames and exercises. In the same vein, no user of cyberpower can have confidence in its use, especially as a coercive agent, unless they test it first. Within the open source environment, the US has yet to *try out* coercion via cyberpower. Instead, the US is reaping the benefits offered by observing and learning from the multiple cyber attack methods being used against it.

Web War I in Estonia

After the collapse of the Soviet Union in 1991, Russian troops did not leave Estonia until 1994.[6] Ever since, Russia has presented to Estonia a deterrent threat of invasion and occupation, and it continues to act in a domineering fashion. According to Harvard University Professor Celeste Wallander, the following negative assessments of NATO enlargement exist among the Russian political elite:

> "For Russia, all the hypothetical security concerns of the past decade are the threats of today. NATO is now closer to Russian borders, and is bombing a non-NATO state. Even before NATO's new strategic concept, the alliance's development of Combined Joint Task Forces offered ways for the alliance to employ forces outside the constraints of Article 5 (self-defense). NATO's changes, combined with its determination to use force against nonmembers threatens Russia because political turmoil in the former Soviet Union increases

[5] See Max Boot, *War Made New: Technology, Warfare, and the Course of History, 1500 to Today*, (New York: Gotham Books, 2006).
[6] CIA, *The World Factbook*, Retrieved from CIA Factbook: https://www.cia.gov/library/publications/the-world-factbook/print/en.html, (accessed: 21 Apr 2009).

> the likelihood of NATO involvement near and perhaps even in Russia. Moscow has long feared that expansion of the alliance could radicalize or destabilize neighboring countries, sparking internal splits or civil wars that could drag in Russia—a role it neither wants nor can afford."[7]

Many members of the new Commonwealth of Independent States (CIS) are keen to shake off the Soviet legacy. The fall-out from this cyber war is unlikely to deter them from further efforts to distance themselves from Moscow's influence. They are bound to continue their quest for independence and international respect.[8] Therefore, fears of neighboring country's independent ambitions may continue to drive Russian actions against states like Estonia and Georgia.

The Estonia case was a failed attempt to use cyberpower to coerce. When the Russian government learned of the Estonian government's plans to move a Soviet-era monument from the center of the capital city, Tallinn, to the suburbs, they clearly warned the Estonian government that removal would be "disastrous" for the Estonians.[9] The Estonians did not comply with the Russian demand and moved the war monument. On the same night that Estonia moved the monument from Tallinn, cyber attacks started against the Estonian cyber infrastructure.

The escalation of the three stages of the cyber attack did not compel the Estonian government to move the war monument back to Tallinn. Coercion against Estonia was attempted via cyberpower in a three-tiered, concerted, and committed approach. This month-long cyber attack in Estonia included tactical (Tier I) script kiddies, operational (Tier II) rogue botnet and zombies, and strategic (Tier III) destruction, denial, and defacement of key government sites and lines of communication in the Estonian cyber infrastructure.[10] Even after enduring over three weeks of cyber attacks, the Estonians did

---

[7] Stephen J. Blank, *Threats to Russian Security: The View from Moscow*, U.S. Army War College, Carlisle, PA, 2000), 3-4.
[8] Kampmark, "Cyber Warfare Between Estonia and Russia," 293.
[9] Hackers Take Down the Most Wired Country in Europe," *Wired Magazine, Issue 15.09*, 21 August 2007, http://www.wired.com/politics/security/magazine/15-09/ff_estonia, (accessed: 28 February 2009).
[10] A hierarchy of cyber threats and capabilities exist: Tier I of "kiddy hackers"-talented, but mostly non-political individuals cracking the net; Tier II include operators with more advanced skills, but with capabilities much less imposing, encompassing, and powerful than those of a nation state; and Tier III which encompasses near-peer competitors with "NSA-like" capabilities plus nation state resources behind them (US, Britain, Russia, China, and a few countries in the EU). See Grant, "Victory in Cyberspace," 26.

not comply with the coercer's demands and did not move the Soviet-era war monument back to its original location in the middle of the capital city.[11]

Ensuing events proved Russian commitment to this conflict. On the morning of 9 May 2007, at the Red Square celebration of the Russian victory over Nazi Germany, President Vladimir Putin proclaimed, "Those who are trying today to… desecrate memorials to war heroes are insulting their own people, sowing discord and new distrust between states and people."[12] This seemed to be a veiled Russian threat. It was followed throughout the day with another 58 separate botnet attacks on Estonian cyber infrastructure.[13] The aggressor's commitment to carry out these attacks was shown through their actions since the cyber attacks continued from 27 April through 9 May 2007.

These cyber attacks included total distributed denial of service (DDoS) attacks across the entirety of the Estonian cyber infrastructure and had potentially strategic effects. These attacks set a precedent. Estonia was the first member state to experience substantial widespread and coordinated attacks on its national cyber infrastructure.[14] These attacks showed the adversary's capability to perform widespread and severe cyber attacks. These attacks could have enabled the adversary to hold the Estonian cyber infrastructure to ransom if the level of punishment inflicted on Estonia was high enough. But, since the effects of the cyber attacks were short-lived and non-consequential, this did not occur. As it was, the Estonians were in the process of discovering counter-cyber attack methods and garnering NATO and EU assistance when the attacks stopped.

Suspicion persists in the international community that Russian intelligence agencies were actively involved in the cyber attacks on Estonia. Further statements from a member of the Russian United Civil Front political party, led by Garry Kasparov, were made, "There is a specific department within the FSB — the successor to the KGB — that specializes in coordinating Internet campaigns against those they consider a threat. They have attacked Chechen rebel sites, us, and now it appears they have attacked

---

[11] See chapter three for expanded discussion.
[12] Hackers Take Down the Most Wired Country in Europe," *Wired Magazine*, *Issue 15.09*, 21 August 2007, http://www.wired.com/politics/security/magazine/15-09/ff_estonia, (accessed: 28 February 2009).
[13] Hackers Take Down the Most Wired Country in Europe," *Wired Magazine*, *Issue 15.09*, 21 August 2007, http://www.wired.com/politics/security/magazine/15-09/ff_estonia, (accessed: 28 February 2009).
[14] Council of Europe, *Cyberterrorism*, (Council of Europe, 2007), 161.

Estonia."[15] If indeed Russian intelligence agencies were actively involved in these attacks, it would prove two facts. One, the Russian government sponsored the attacks. Two, the Russian government premeditated cyber attacks against another state.

The future impact of the cyberpower used to coerce Estonia is uncertain. Estonia is a highly cyber-dependent, paperless society, and can consequently be "cyber-locked" in the same way some countries are landlocked.[16] The main operational objective of these politically motivated cyber attacks seemed to be "cyber-locking" Estonia by shutting down its cyber infrastructure.[17] To explain "cyber-locked," if a country cannot use its cyber-infrastructure, cyber attacks will have greater coercive potential. In essence, by taking command and control of a country's cyber infrastructure at will, an adversary could hold it to ransom. Of course, the level of coercive effectiveness an act like this has depends on how much value that country puts on its cyber infrastructure. When the total shutdown of the Estonian cyber infrastructure occurred, it severely affected the entire Estonian society. They could not conduct Internet-based operations, communicate via e-mail or VoIP, and many telephone systems were inoperative. The Estonian Parliaments' means of communication (e-mail and Internet) and all online news sites were shutdown and over 90 percent of Estonian online banking and Automatic Teller Machine systems were also shutdown.[18] In the future, this could make cyber attack more likely and effective since it demonstrated the impact that cyber attacks can have on a highly cyber-dependent country. This could bolster credibility of future cyber threats, unless Estonia increases the defense and security capabilities of its cyber infrastructure. These events advertised certain methods of cyber attack. In the future, this could make similar attacks more difficult as states redouble their cyber infrastructure defenses and security.

Cyber Attacks on Georgia

The attacks on the Republic of Georgia were both cyber and physical, of which cyberpower's actual level of contribution is difficult to assess. This combined arms cyber

---

[15] Grant, "Victory in Cyberspace," 4.
[16] Associated Press, *Estonia Blazes Internet Trail,* "New York Times.com," http://files.wifi.ee/nytimes.pdf, (accessed: 21 April 2009).
[17] Centre of Excellence Defence Against Terrorism, N. P. (2008). *Responses to Cyber Terrorism.* New York, NY: IOS Press, 98.
[18] Hackers Take Down the Most Wired Country in Europe," *Wired Magazine, Issue 15.09,* 21 August 2007, http://www.wired.com/politics/security/magazine/15-09/ff_estonia, (accessed: 28 February 2009).

and physical attack sought to wrest control of Georgian territories by brute force. The cyber attacks on Georgia were arguably a success as they proved possible the potential of cyberpower being used to supplement kinetic actions. Yet, it is difficult to decipher how much of the Russian success to force Georgian capitulation was due to cyberpower. All the same, it remains certain that Russia would have achieved its objectives without cyberpower.

Since the cyber attacks started before the physical attacks, it is possible that the use of cyberpower was an attempt by Russia to force the Georgians to relinquish their territories and capitulate prior conducting acts of brute physical force. In the Georgian case, even though the cyber attacks did occur prior to the physical attacks, there was no threat issued before the cyber attacks commenced. There was no threat or demand issued so, the cyber attacks cannot be interpreted as an attempt of coercion. The cyber attacks started on 19 July 2008. No bombs dropped or tanks rolled until after 7 August 2008 while. An increase of cyber attacks was noted on 8 August 2008. This might have been because the Russians wanted to try to force Georgian capitulation with a low cost method (cyber attack) prior to moving to a high cost method (tanks and troops). The increased cyber attacks on 8 August hampered Georgian command and control at a critical time just after Georgian armed forces engaged Russian forces on 7 August 2008.

During the Georgian cyber attacks examples of coercion theory present themselves, but since the aggressor has not taken accountability for the attacks, they actually exemplify brute force more than coercion. Successful coercion includes a threat of action or continued action. The credibility of a threat is based on communication, capability, and commitment. The threat in the Georgian case could be interpreted as the Russian government announcing their continued backing of the separatist regions of South Ossetia and Abkhazia.[19] But, the Russian government was not reported to have directly said that Georgia must give up its rights to South Ossetia and Abkhazia, otherwise its cyber infrastructure might have been attacked until it complied. Since there was no clear threat reported of this type, it is highly unlikely that the Russian cyber attacks were an attempt at coercion. The fact, however, that the attacks lasted for the

[19] The New York Times, "Abkhazia and South Ossetia: Differences Matter," 12 August 2008, *New York Times.com,* *http://topics.blogs.nytimes.com/2008/08/12/abkhazia-and-south-ossetia-differences-matter/?scp=3&sq=south%20ossetia%20war&st=cse*, (accessed: 2 June 2009).

better part of a month at least demonstrated commitment. These cyber attacks cut Internet access, stopped cell phone communications, and denied service to Georgian government e-mail servers and Internet-based applications. This handcuffed some of the government's command and control capability, which might have facilitated Russian kinetic actions during the South Ossetian War of 2008. The Russian government has not taken accountability for the cyber attacks conducted on Georgia. Unless an aggressor becomes accountable, these attacks technically cannot be seen as an example of coercion. Coercion requires it to be clear who is the coercer and coercee. In this case, the obvious coercee is Georgia. The Grey Goose Reports were unable to make any direct references to Russian state organizations guiding or directing these attacks.[20] At this time, it cannot be irrefutably concluded that the Russian government was responsible for the attacks. There is no evidence of the attacks being conducted for coercive purposes. Therefore, the cyber attacks exemplified cyberpower being used in brute force actions more than coercive actions.

One cannot quantify the extent of cyberpower's contribution to the Russian conquest and occupation of parts of Georgia. Notwithstanding, one can say that the cyber attacks that preceded the brute force physical actions taken by Russian armed forces effectively shut down normal Georgia government operations and frustrated the government's ability to coordinate effective defenses against the Russian invading and occupying forces. The time, effort, and resources spent on the cyber attacks hampered the Georgian government's ability to resist aggressive Russian threats of invasion and acts of occupation. These cyber attacks – along with physical attacks – prevented the Georgian government from being able to plan, communicate, and coordinate effectively with Georgian armed forces and civilians. These combined attacks induced the Georgians to withdraw its forces from the disputed territory.[21]

In the end, the increased costs of continued resistance induced Georgian compliance with Russian demands. Cyberpower – combined with physical force –

[20] Project Grey Goose Report: Phase I, 17 October 2008, http://www.scribd.com/doc/6967393/Project-Grey-Goose-Phase-I-Report#document_metadata, (accessed: 4 March 2009) and Grey Goose Report: Phase II Report, 20 March 2009, http://greylogic.us/?page_id=85, (accessed: 24 May 2009).
[21] Based on discussion and references in chapter four.

demonstrated the ability to impose costs on a government. This demonstration could help make future cyber threats credible as coercive tools.

To put the Estonia and Georgia cases in context, the long-term damage caused from the cyber attacks was minimal. E-mail was disrupted, Internet access, some telecommunications, and emergency services were denied, but little permanent damage ensued from the attacks. Since Georgia's government relied less on the Internet for normal operations than Estonia, the short-term negative effect from these cyber attacks was also lessened.[22]

Cyberpower's Shortcomings

Cyberpower has shortcomings as a coercive instrument. Any serious analysis of using cyberpower as a manipulative agent must take into account its drawbacks. These are directly associated with establishing threat credibility in deterrent and compellent actions. They include the ease of producing countermeasures and political and economic implications of use.

To use cyberpower for deterrence or compellence requires cyberpower to serve as the basis for a credible threat. The ease of producing countermeasures hampers this action.[23] The anonymous and ubiquitous nature of cyberspace makes threats difficult to trace and attribute.[24] Like many things in cyberspace, it is often difficult to determine who is on the other end. Specific cyber capabilities are generally lost once exposed, so a threat cannot be too specific. Prior attacks may not prove credible because the specific method of cyber attack that was successful in the past may not be unbeatable in the future.

The ability to quickly create countermeasures means that cyberpower lacks persistence. In the Georgia case, the government "turned to using the Google Blogger service as a method of communication…and it has proved to be a sustainable resource."[25] By doing this, Georgia maneuvered in the midst of cyber attack by

[22] "Marching Off to Cyberwar," *The Economist Technology Quarterly*, 6 December 2008, 20-21.
[23] This concept discussed during personal interview with FBI Cyber Investigation Joint Task Force Director, 1 April 2009, Washington, DC.
[24] This concept discussed during personal interviews with six CIA Cyber Investigation Special Task Force members, 31 March 2009, Langley, VA.
[25] Korns and Kastenberg, "Georgia's Cyber Left Hook," 67-68.

relocating its strategic Internet-based cyber capabilities to America. This had the operational effect of ensuring continued command and control capabilities between the Georgian government and its armed forces and civilian populace. This resulted in a partial defeat of the cyber attacks.[26] It had the strategic effect of undermining the long-term power of these attacks, but unfortunately for Georgia, not quickly enough. Ultimately, the cyber attack methods used were only viable for short-term use with short-term effects. Even though they may be short lived, cyber attacks can carry unknown political and economic effects and implications.

Political and economic implications can arise when using cyberpower to coerce. What direct effects from cyber attacks could severely affect the image of a political leader? If a political leader's image is damaged because of bad press caused from cyber attacks, as happened to Georgian President Saakashvili's website, it could undermine support for that leader. If enough support for a leader is undermined, it can cause the leader to lose office. What are the unintended effects from an economic downturn caused by cyber attacks? There are a myriad of unknown negative economic effects from cyber attacks on financial institutions. If commercial and personal finances are siphoned away, this could cause widespread financial devastation for industries and society at large. If trust in banking institutions is lost because the banks cannot control their data and information, the economic base for society will be severely affected. If both companies and individuals do not have a place to safely store their money or borrow money, the ability for society to operate normally will be diminished. These questions need consideration prior to using cyberpower to coerce for political or economic gain.

Cyberpower's Potential

Cyberpower has demonstrated potential as a coercive instrument. It is possible for cyberpower to be used in coercive efforts and the potential exists to cripple a nation. All that stops an adversary from roaming free in cyberspace is general Internet, network, and computer security. This can mean anything from a rudimentary password system to a costly array of firewalls that electronically block access to a system. A country's critical computer, telecommunication, and civil infrastructures are open to any adversary

[26] Korns and Kastenberg, "Georgia's Cyber Left Hook," 67-68.

who finds the right keys. Adversaries can hold cyber infrastructures for ransom until the coercee complies with demands. Low costs and quick employment can make brute force cyber attacks advantageous in comparison to other coercive acts.

Coercion is the manipulation of an enemy's cost-benefit calculus so as to lead the target entity to make the choices that the coercer desires. When a target entity has no choice and the preference is achieved directly by brute force, coercion is no longer at play. Brute force is generally more costly than coercion, be it deterrence or compellence, in regards to kinetic force. On the other hand, when it comes to cyber, brute force may be the best method to use where it is technically feasible. Brute force does not rely on communicating a threat or establishing credibility, and therefore does not provide an enemy the opportunity beforehand to develop countermeasures. Brute force cyber attacks do not expend tangible assets. The increasing control of the physical realm by cyber systems increases the potential to exert physical control via cyberpower.

Cyberpower has the potential to deal great punishment on an adversary. Cyber infrastructures derive value from interconnectedness. However, the interconnectedness and contiguous nature of cyberspace provides inherent weakness and openness to attack. Even non-Internet, non-contiguous systems are still reachable. Removable media, embedded hardware, and insiders can implant the means of attack.

Cyberpower can have a heavy impact. In a brute force cyber attack, the possibilities are endless as to what public systems could be shut down, manipulated, or controlled quickly and without prior notice. Worst case, there would be no Internet, no transportation, no communications, no power, no water, no money, no records, and no identity. This scenario could carry heavy effects to any society.

Conclusion

There are various ways to use cyberpower to coerce. The potential exists to cripple a nation, as the DDoS attacks against Estonia's banking system proved. But, the ways that cyberpower can be employed still require development to become reliable and effective in successful manipulative efforts against countries and non-state actors. The murky realm of cyberspace includes unknown and possibly unacceptable consequences. Several precedents have been set, including the precedent to use cyberpower to attack a

state, the use of cyberpower in a premeditated cyber-only attack, and the combination of cyber attacks and military force. Cyber attacks within open networks have proved that they can create far-reaching collateral damage and effects.

This chapter evaluated the case studies in terms of the coercion theory explained in chapter one. The US cases provided useful information about uses of cyberpower, but did not satisfy coercion theory. Coercion was attempted but unsuccessful in the Estonia case, where it set a precedent for cyber attack against a state. Georgia's case also set precedent with simultaneous premeditated cyber and physical attacks against a country, but cyberpower's contribution to military effectiveness is unclear. Overall, cyberpower still has shortcomings as a coercive instrument.

Capabilities exist to make cyberpower an effective coercive instrument. At the present time, these capabilities do not inflict enough punishment to be singularly effective at coercion. Cyberpower shows the potential to hurt an opponent and is most likely to achieve strategic effects when combined with other instruments of power. There is no evidence, however, that as societies become more reliant on cyber infrastructure, that cyberpower cannot become an effective coercive instrument on its own.

Conclusion

The study of coercion via cyberpower is an intellectually tough subject to comprehend, let alone examine. Cyberpower failed to deter or compel in the cases examined. The research question of this study asked, "Can cyberpower coerce adversarial states and non-state actors?" This thesis concludes that *used alone, cyberpower has yet to show coercive ability. Used in a combined campaign with other instruments, it also has yet to prove its coercive ability. However, cyberpower can be effective in brute force actions, both alone and when combined with other instruments.* It remains difficult to tell how much cyberpower contributes compared with physical forces in a combined campaign. In the cases studied here, it showed potential as an effective coercive instrument, but it was not persistent and powerful enough to prove itself.

Chapter one described cyber terms relevant to this study. When attempting to coerce using cyberpower, it is important to have a baseline understanding of cyber, cyberspace, cyber infrastructure, cyberpower, and cyber warfare. Chapter one parsed the basic pieces of coercion theory. It defined deterrence and compellence. Chapter one also discussed the closely related concept of brute force.

Chapter two examined the prominent features of over a decade's worth of cyber attacks against the US. The details of Solar Sunrise, Code Red, Mountain View, Nimda, Slammer, Titan Rain, and Conficker provide a good overview of how cyberpower can potentially be used to inflict punishment. The motive and object of these attacks are still unknown. It remains unclear as to if these attacks were failed attempts at coercion or just meant to be operational tests and demonstrations of capability.

Chapter three showed that cyber-dependent nations like Estonia are vulnerable to cyber warfare. The Estonia attack most likely shook more nerves than it caused long-term damage. However, it set a precedent for cyber warfare applied against a state. It also created profound questions about what qualifies as war in cyberspace. The cyber attacks on Estonia had much clearer motive, objective, and organization than the attacks on the US.

Chapter four examined the premeditated combined cyber-physical attack campaign on Georgia leading to Russian military occupation of disputed separatist

territories. It is unknown what cyberpower actually contributed to this campaign. It was the first case of cyberpower combined with armed force in a premeditated and successful campaign. These cases demonstrate that cyber attack is becoming more common, but institutions that help manage conflict have yet to catch up.

Chapter five analyzed the cases through the coercion framework set forth in the first chapter. Conclusions about the use of cyberpower as a coercive instrument include:

- Coercion via cyberpower has been attempted, but so far, unsuccessfully.
- Cyberpower shows a great deal of potential as a coercive instrument.
- Cyberpower can be exercised through a wide range of methods.
- Cyberpower still has shortcomings as a coercive instrument.
- Cyberpower needs development to be reliable and capable.
- Cyberpower needs further evolution to increase its potential to punish.
- Cyberpower has been integrated into a combined arms campaign.
- Cyberpower may be effective when combined with other instruments, although it is difficult to determine how effective.
- Cyber attacks can have wide-ranging unintended consequences, and therefore must be carefully focused.
- The precedent of premeditated cyber warfare has been made.

The challenges of using cyberpower as a coercive instrument are many. Cyberpower today is often seen only as an enabler to net-centric warfare, not as a tool of warfare in itself.[1] Another challenge of using cyberpower is that it has no set geographical boundaries. Therefore, cyber attacks can have second, third, and fourth order effects that make it difficult to use without fear of response in kind from other parties – possibly felt around the globe. Additionally, how much or how little a target responds to coercive or brute force uses of cyberpower can depend on the level of cyber dependency of the target.

Though cyberpower has had little effect thus far as a coercive instrument, this may change as societies become more cyber-reliant. The United States and Estonia have become dependent on cyberpower. If a country becomes "cyber-locked" in the same way that countries are land-locked, cyber attacks will have greater coercive capability. The strategic effectiveness of cyber attacks is directly linked to how much or how little the

[1] This concept derived from personal interview with the Commander of the USAF Gunter AFB, AL, Network Operations Center (NOC), 26 April 2009, Montgomery, AL.

target relies on its cyber infrastructure. The strategic implications of this dependence are just beginning to be appreciated.

As with airpower in 1918, the strategic effects and implications of coercing via cyberpower remain largely undiscovered and unproven. The destruction that kinetic attacks bring cannot usually be undone in a short period of time. Conversely, the damage from many forms of cyber attack is temporary. For example, denial of service cyber attacks are likely to inflict short-term damage, and can be reversed as soon as the attacks stop. The damage caused by lost productivity from denial of services, however, is more difficult to calculate. All the same, most denial of service damage is reversible as soon as services are accessible.

Cyber attacks might be able to achieve strategic results without physical damage and the ensuing political backlash. Cyberpower could be a very surgical coercive instrument. Nevertheless, strategies employing cyberpower require its use to be studied in much greater detail prior to employment because cyberpower also has the potential to generate widespread unintended consequences. A cyber attacker would also need to be prepared for a cyber counter-attack.

This field is ripe for more study. A classified version of this study would be able to offer much greater detail. The limits of an open source study on such a close-hold topic are challenging at best. Legal aspects of cyberspace operations should be studied to include defensive and offensive actions – a plethora of legal issues can stem from cyber attacks. A study examining the most strategically effective methods of cyber attack would be of great value. A study examining the best methods of counter-cyber attack is also needed. Cyberpower as a coercive instrument has endless possibilities, but we have only scratched the surface in thinking through the methods, defenses, and implications.

Coercion via cyberpower opens a vast new area of operations. Cyberspace dominates the global commons more and more each day. At present, there are endless possibilities to prove cyberpower's use as an effective coercive agent, but they need to be tested and proven. Nevertheless, the use of cyberpower as a coercive agent is within reach. Cyberpower shows strong potential to coerce a target resulting in the achievement of strategic objectives, when employed smartly as a part of a well-crafted strategy.

BIBLIOGRAPHY

Academic Papers

Arwood, Samuel. "Cyberspace as a Theater of Conflict: Federal Law, National Strategy and The Departments of Defense and Homeland Security" Graduate Research Project, Wright-Patterson Air Force Base, OH: Air Force Institute of Technology, Department of Electrical and Computer Engineering, 2007.

Billo, Charles. Change, Welton. "Cyber Warfare: An Analysis of the Means and Motivation of Selected Nation States" Master's thesis, Dartmouth College, 2004.

Blank, Stephen J. "Threats to Russian Security: The View from Moscow" Master's thesis, U.S. Army War College, 2000.

Franz, Timothy P. "IO Foundations to Cyberspace Operations: Analysis, Implementation Concept, and Way-Ahead for Network Warfare Forces" Master's thesis, Air Force Institute of Technology, 2007.

Williams, Paul D. "USAF Cyber Capability Development: A Vision for Future Cyber Warfare & A Concept for Education of Cyberspace Leaders" Research Paper, Air Command and Staff College, 2009.

Articles

Abraham, Peter. "The Slammer Worm Attack: The worst attack to date, probably not the last." *Dynamic.net News*, 14 February 2003, http://dynamicnet.net/news/articles/slammer.html (accessed 5 March 2009).

Adair, Steven. "Georgian Websites Under Attack - DDoS and Defacement." *Shadowserver,* 11 August 2008, http://www.shadowserver.org/wiki/pmwiki.php?n=Calendar.20080811 (accessed 4 March 2009).

Alison, Sebastian and Pronina, Lyubov. "Russia Recognizes Independence of Georgian Regions." *Bloomberg.com*, http://www.bloomberg.com/apps/news?pid=20601082&sid=afAvlgTbOoAg&refer=canada (accessed 11 April 2009).

Associated Press. "Estonia Blazes Internet Trail." *New York Times.com*, http://files.wifi.ee/nytimes.pdf (accessed 21 April 2009).

BBC News. "Georgia and Russia agree on truce." *BBC news.com,* 13 August 2008, http://news.bbc.co.uk/2/hi/europe/7557457.stm (accessed 21 April 2009).

BBC News. “Timeline: The Conficker Worm.” 31 March 2009, http://news.bbc.co.uk/2/hi/technology/7973829.stm (accessed 4 April 2009).
BBC News. “Clock ticking on worm attack code.” 20 January 2009, *BBC.com*, *http://news.bbc.co.uk/1/hi/technology/7832652.stm* (accessed 12 May 2009).

Clements, Matthew, “Georgia Launches Major Assault on South Ossetia.” Janes.com, 8 August 2008, http://www.janes.com/media/releases/pc080808_2.shtml (accessed 24 May 2009).

“Coordinated Russian vs Georgia Cyber Attack in Progress.” *ZDNet*, http://blogs.zdnet.com/security/?p=1670 (accessed 4 March 2009).

“Cyber War!” *Frontline.com*, 18 March 2003, http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/warnings/ (accessed 5 March 2009).

Gellman, Barton. “Cyber-Attacks by Al Qaeda Feared.” *The Washington Post.com*, 27 June 2002, http://www.washingtonpost.com/wpdyn/content/article/2006/06/12/AR2006061200711.html (accessed 11 May 2009).

“The Cyber Raiders Hitting Estonia.” *BBC News*, International Version, 17 May 2007, http://news.bbc.co.uk/2/hi/europe/6665195.stm (accessed 28 February 2009).

“A Cyber-riot.” *The Economist*, 12 May 2007, Vol 383 Issue 8528.

Danchev, Dancho. “Georgia President’s web site under DDoS Attack from Russian hackers.” *zdnet.com*, 22 July 2008, http://blogs.zdnet.com/security/?p=1533 (accessed 21 April 2009).

“Estonia Pulls Off Nationwide Net Voting.” *CNET News*, 19 October 2005, http://news.cnet.com/Estonia-pulls-off-nationwide-Net-voting/2100-1028_3-5898115.html (accessed 28 February 2009).

Evron, Gadi. “Battling Botnets and Online Mobs - Estonia's Defense Efforts during the Internet War.” *Science & Technology*, Winter/Spring 2008.

Gearan, Anne. “Georgia’s oil pipeline is key to US support.” *San Francisco Chronicle.com*, 9 August 2008, http://www.sfgate.com/sports/preps/ (accessed 7 May 2009).

“Georgia Withdraws, Russia Presses for Attack.” *Wired*, http://blog.wired.com/defense/2008/08/georgian-troops.html (accessed 4 March 2009).

Grant, Rebecca. "Victory in Cyberspace." Air Force Association, 2007.

"Hackers Take Down the Most Wired Country in Europe." *Wired Magazine, Issue 15.09,* 21 August 2007, http://www.wired.com/politics/security/magazine/15-09/ff_estonia (accessed 28 February 2009).

Jaffe, Greg. "Gates Urges NATO Ministers to Defend Against Cyber Attacks." *Wall Street Journal,* 15 June 2007.

Kampmark, Binoy. "Cyber Warfare Between Estonia and Russia." *Contemporary Review*, Autumn 2007, 293.

Korns, Stephen W. and Kastenberg, Joshua E. "Georgia's Cyber Left Hook." *Parameters,* Winter 2008-09, 60-73.

Lesk, Michael. "The New Front Line: Estonia under Cyberassault." *IEEE Security and Privacy*, vol. 5, no. 4, pp. 76-79, July/Aug. 2007, http://www2.computer.org/portal/web/csdl/doi/10.1109/MSP.2007.98 (accessed 2 May 2009).

Lewis, James A. "Cyber Attacks Explained." *Center for strategic and International Studies,* 15 June 2007, http://www.csis.org/media/csis/pubs/070615_cyber_attacks.pdf (accessed 29 April 2009).

"Marching Off to Cyberwar." *The Economist Technology Quarterly*, 6 December 2008, 20-21.

Markoff, John. "Worm Infects Millions of Computers Worldwide." *CNET.com*, 22 January 2009, http://www.nytimes.com/2009/01/23/technology/internet/23worm.html?_r=1&em\ (accessed 8 April 2009).

Mills, Elinor. "FAQ: Conficker time bomb ticks, but don't expect boom." *CNET com,* 25 March, 2009, http://news.cnet.com/faq-conficker-time-bomb-ticks-but-dont-expect-boom (accessed 8 April 2009).

Mills, Elinor. "Researchers say Conficker is all about the money." *CNET.com*, http://news.cnet.com/8301-1009_3-10216205-83.html (accessed 9 April 2009).

Moore, David and Shannon, Colleen. "The Spread of the Code Red Worm." *CAIDA: The Cooperative Association for Internet Data Analysis,* 18 November 2008, http://www.caida.org/research/security/code-red/coderedv2_analysis.xml (accessed 8 March 2009).

Myers, Steven Lee. "Estonia Computers Blitzed, Possibly by the Russians." *New York Times*, 19 May 2007, http://www.nytimes.com/2007/05/19/world/europe/19russia.html?fta=y (accessed 1 March 2009).

Onley, Dawn S. and Wait, Patience. "Red Storm Rising," *GCN.com*, 17 August 2006, http://gcn.com/articles/2006/08/17/red-storm-rising.aspx (accessed 28 March 2009).

Reuters, "FACTBOX-Key Facts on Rebel Region of South Ossetia." *Reuters.com*, 31 May 2009, http://www.reuters.com/article/asiaCrisis/idUSLV15723 (accessed 31 May 2009).

Ryan, Justin, "Conficker Conflunks." *Linux Journal*, 2 April 2009, http://www.linuxjournal.com/content/conficker-conflunks (accessed 12 May 2009).

Ryan, Justin. "Newstradamus Reports: Navy Nailed by Virus." *Linux Journal*, 19 January 2009, http://www.linuxjournal.com/content/newstradamus-reports-navy-nailed-virus (accessed 12 May 2009).

"Solar Sunrise." *Global Security Organization*, http://www.globalsecurity.org/military/ops/solar-sunrise.htm (accessed 11 April 2009).

Stahl, Leslie. "The Conficker Worm: What Happens Next? 60 Minutes: Computer Worm Could Receive New Instructions On April 1." *60 Minutes, CBS.com*, 29 March 2009, http://www.cbsnews.com/stories/2009/03/27/60minutes/main4897053.shtml (accessed 30 March 2009).

Sterling, Bruce. "Estonia: NATO's Brand New Center of Cyberwarfare Excellence." *WIRED.com*, 30 April 2008, http://www.wired.com/beyond_the_beyond/2008/04/estonia-natos-b/, (accessed 4 June 2009).

The New York Times, "Abkhazia and South Ossetia: Differences Matter." 12 August 2008, *New York Times.com*, *http://topics.blogs.nytimes.com/2008/08/12/abkhazia-_and-south-ossetia-differences matter/?scp=3&sq=south%20ossetia%20war&st=cse* (accessed 2 June 2009).

Torbakov, Igor. "The Georgia Crisis and Russia-Turkey Relations." *The Jamestown Foundation*, http://www.jamestown.org/programs/recentreports/single/?tx_ttnews%5Btt_news%5D=34181&tx_ttnews%5BbackPid%5D=7&cHash=12982f773b (accessed 4 March 2009).

Thornburgh, Nathan. “Inside the Chinese Hack Attack.” *Time* , 25 August 2005, http://www.time.com/time/nation/article/0,8599,1098371,00.html (accessed 28 March 2009).

Wright Squawks. “French fighter aircraft grounded by virus attack.” 11 February 2009, http://wrightsquawks.blogspot.com/2009/02/french-fighter-aircraft-grounded-by.html (accessed 12 May 2009).

Books

The American Heritage Dictionary of the English Language, Fourth Edition, Boston, MA: Houghton Mifflin Company, 2004.

Art, Robert J., “To What Ends Military Power?”, *in* Paul J. Bolt, Damon V. Coletta, Collins G. Shackelford, *American Defense Policy*, Baltimore, MD: JHU Press, 2005.

Beale, Jay; Caswell, Brian; Foster James C.; Posluns, Jeffrey; and Russell, Ryan. *Snort 2.0 Intrusion Detection*, Rockland, MA: Syngress, 2003.

Bidgoli, Hussein. *Handbook of Information Security: Threats, Vulnerabilities, Prevention, Detection, and Management*, Hoboken, NJ: John Wiley and Sons, 2006.

Boot, Max. *War Made New: Technology, Warfare, and the Course of History, 1500 to Today*, New York: Gotham Books, 2006.

Broadhurst, Roderic G. and Grabosky, Peter N. *Cyber-crime*, Hong Kong: Hong Kong University Press, 2005.

Byman, Daniel, and Waxman, Matthew C.. *The Dynamics of Coercion: American Foreign Policy and the Limits of Military Might*, Rand Studies in Policy Analysis. Cambridge: Cambridge University Press, 2002.

Contos, Brian T. *Enemy at the water cooler,* St Louis, MO: Elsevier Press, 2006.

Council of Europe. *Cyberterrorism*, Council of Europe: 2007.

Dunnigan, James F. *The next war zone*, Charleston, SC: Citadel Press, 2003.

Forest, James J. *Homeland Security: Critical Infrastructure*, Westport, CT: Greenwood Publishing Group, 2006.

Freedman, Lawrence. *Deterrence*. Cambridge: Polity Press, 2004.

Freedman, Lawrence. *Strategic Coercion: Concepts and Cases*, Oxford: Oxford University Press, 1998.

Janczewski, Lech and Colarik, Andrew M. *Cyber Warfare and Cyber Terrorism*, Hershey, PA: Idea Group Inc, 2007.

Libicki, Martin C. *Conquest in Cyberspace: National Security and Information Warfare*. New York, NY: Cambridge University Press, 2007.

Liska, Allan. *The Practice of Network Security*, Upper Saddle River, NJ: Prentice Hall PTR, 2003.

Lucas, Edward. *The New Cold War: Putin's Russia and the Threat to the West*, New York: Palgrave Macmillan, 2008.

Moran, Daniel and Russell, James A. *Energy and Global Politics*, London, UK: Taylor and Francis, 2008.

Notholt, Stuart. *Fields of Fire: An Atlas of Ethnic Conflict*, Kibworth Beauchamp, Leicester: Troubador Publishing Ltd., 2008.

Pape, Robert Anthony. *Bombing to Win: Air Power and Coercion in War*, Cornell Studies in Security Affairs. Ithaca, N.Y.: Cornell University Press, 1996.

Pollack, Kenneth M.. *The Threatening Storm: The Case for Invading Iraq*, New York: Random House, 2002.

Ragaini Richard C. *International Seminar on Nuclear War and Planetary Emergencies — 38th Session*, Singapore: World Scientific, 2008.

Rattray, Gregory J. *Strategic Warfare in Cyberspace*, Cambridge, MA: MIT Press, 2001.

Schell, Bernadette Hlubik and Martin, Clemens. *Cybercrime*, Oxford, UK: ABC-CLIO, 2004.

Schelling, Thomas C. *Arms and Influence*, London: Yale University Press, 1966.

Schiller, Craig A. Binkley, Jim. Harley, David. Evron, Gadi. Bradley, Tony. *Botnets*, New York: Syngress, 2007.

Tipton, Harold F. and Krause, Micki. *Information Security Management Handbook, Edition: 6*, Boca Raton, FL: CRC Press, 2007.

Toffler, Alvin and Heidi. *War and Anti-War: Survival at the Dawn of the 21st Century*, London: Little, Brown, 1993.

Verton, Dan, *Black Ice: The Invisible Threat of Cyber-Terrorism*, Emeryville, CA: McGraw-Hill/Osborne, 2003.

Weimann, Gabriel, *Terror on the Internet: The New Arena, the New Challenge*, Washington, DC: US Institute for Peace, 2006.

Zichichi, Antonino, Ragaini, Richard C., and Majorana, Ettore. International Centre for Scientific Culture. *International Seminar on Nuclear War and Planetary Emergencies*, Hackensack, NJ: World Scientific, 2004.

Electronic Publications

"About.com: Internet Security, 'bots and zombies'." http://netsecurity.about.com/od/frequentlyaskedquestions/qt/pr_bot.htm (accessed 29 March 2009).

"Encarta World English Dictionary [North American Edition]." http://encarta.msn.com/artcenter_/browse.html (accessed 5 May 2009).

"Infoplease Online Encyclopedia." http://www.infoplease.com/encyclopedia/ (accessed 1 March 2009).

"US Central Intelligence Agency, The World Factbook." https://www.cia.gov/library/publications/the-world-factbook/ (accessed 5 May 2009).

Government Documents

"Air Force Doctrine Document 2-11, Cyberspace Operations." Air Force Doctrine Center, 2008.

CRS Report for Congress. "Russia-Georgia Conflict in South Ossetia: Context and Implications for U.S. Interests." Washington, DC: US Congress, 2008.

Jabbour, Dr. Kamal T. *50 Cyber Questions Every Airman Can Answer*, Air Force Research Laboratory, 2008

"Joint Publication, 3-13, Information Operations." Washington D.C.: Joint Staff, 2006.

Resolution of the Parliament of Georgia on the Occupation of the Georgian Territories by the Russian Federation, http://www.parliament.ge/index.php?lang_id=ENG&sec_id=98&info_id=20047, (accessed: 1 March 2009).

"The White House, The National Strategy to Secure Cyberspace." Washington DC: Office of the President of the United States, 2003.

US Department of Defense. *Air Force Cyber Command Strategic Vision*. Washington D.C.: Joint Staff, 2007.

US Department of Defense. *National Military Strategy for Cyberspace Operations.* Washington D.C.: Joint Staff, 2006.

Reports

Centre of Excellence Defence Against Terrorism, N. P. *Responses to Cyber Terrorism.* New York, NY: IOS Press, 2008.

Project Grey Goose. Report: Phase I, 17 October 2008, http://www.scribd.com/doc/6967393/Project-Grey-Goose-Phase-I-Report#document_metadata (accessed: 30 March 2009).

Swedish Emergency Management Agency. *Large Scale Internet Attacks, The Internet Attacks on Estonia,* Huskvarna: Swedish Emergency Management Agency, 2008.